Configuring Traffic Filters and Protocol Prioritization

Router Software Version 11.0
Site Manager Software Version 5.0

Part No. 114081 Rev. A
August 1996

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1988–1996 Bay Networks, Inc.

All rights reserved. Printed in the USA. August 1996.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notice for All Other Executive Agencies

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Trademarks of Bay Networks, Inc.

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, Optivity, PPX, SynOptics, SynOptics Communications, Wellfleet and the Wellfleet logo are registered trademarks and ANH, ASN, Bay•SIS, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, PathMan, PhonePlus, Quick2Config, RouterMan, SPEX, Bay Networks, Bay Networks Press, the Bay Networks logo and the SynOptics logo are trademarks of Bay Networks, Inc.

Third-Party Trademarks

All other trademarks and registered trademarks are the property of their respective owners.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks Software License

Note: This is Bay Networks basic license document. In the absence of a software license agreement specifying varying terms, this license -- or the license included with the particular product -- shall govern licensee's use of Bay Networks software.

This Software License shall govern the licensing of all software provided to licensee by Bay Networks ("Software"). Bay Networks will provide licensee with Software in machine-readable form and related documentation ("Documentation"). The Software provided under this license is proprietary to Bay Networks and to third parties from whom Bay Networks has acquired license rights. Bay Networks will not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either Software or for a Bay Networks product ("Equipment") that is packaged with Software. Each such license is subject to the following restrictions:

1. Upon delivery of the Software, Bay Networks grants to licensee a personal, nontransferable, nonexclusive license to use the Software with the Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such Equipment and to such facility. Software which is licensed for use on hardware not offered by Bay Networks is not subject to restricted use on any Equipment, however, unless otherwise specified on the Documentation, each licensed copy of such Software may only be installed on one hardware item at any time.
2. Licensee may use the Software with backup Equipment only if the Equipment with which or for which it was acquired is inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Neither title nor ownership to Software passes to licensee.
6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors, or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.
7. Third-party owners from whom Bay Networks has acquired license rights to software that is incorporated into Bay Networks products shall have the right to enforce the provisions of this license against licensee.
8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret, or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensee as permitted by this license.

Bay Networks Software License *(continued)*

9. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software. [Note: For licensees in the European Community, the Software Directive dated 14 May 1991 (as may be amended from time to time) shall apply for interoperability purposes. Licensee must notify Bay Networks in writing of any such intended examination of the Software and Bay Networks may provide review and assistance.]
10. Notwithstanding any foregoing terms to the contrary, if licensee licenses the Bay Networks product "Site Manager," licensee may duplicate and install the Site Manager product as specified in the Documentation. This right is granted solely as necessary for use of Site Manager on hardware installed with licensee's network.
11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Bay Networks may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Bay Networks. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and Documentation, including all copies, to Bay Networks.
12. Licensee's obligations under this license shall survive expiration or termination of this license.

Contents

Configuring Traffic Filters and Protocol Prioritization

About This Guide

Before You Begin xv
Conventions xvi
Acronyms xvii
Ordering Bay Networks Publications xviii

Technical Support and Online Services

Bay Networks Customer Service xx
Bay Networks Information Services xxi
World Wide Web xxi
Customer Service FTP xxi
Support Source CD xxii
CompuServe xxii
InfoFACTS xxiii
How to Get Help xxiii

Chapter 1
Using Traffic Filters

What Are Traffic Filters? 1-1
Inbound Traffic Filters 1-2
Outbound Traffic Filters 1-3
What Is Protocol Prioritization? 1-3
DLSw Prioritization Filters 1-4
What Do Traffic Filters Do? 1-5
Ensure Consistent Service 1-5
Reduce Network Congestion 1-5
Prioritize Important Traffic 1-5
Reduce Loss of Critical Data 1-5

Enhance Security 1-5
Filtering Strategies 1-6
Drop or Accept Certain Traffic 1-6
Build a Firewall 1-6
Direct Certain Traffic 1-6
Combine Filters 1-7
Components of Traffic Filters 1-7
Criteria 1-8
Predefined and User-Defined Criteria 1-9
User-Defined Criteria 1-12
Ranges 1-12
Actions 1-13
Filtering Actions 1-13
Prioritizing Actions 1-14
Dial Service Actions 1-14
Using Filter Templates 1-15
Creating a Template 1-16
Traffic Filter Summary 1-17

Chapter 2
Using Protocol Prioritization

About Priority Queues 2-2
The Dequeuing Process 2-2
Bandwidth Allocation Algorithm 2-3
Strict Dequeuing Algorithm 2-6
Tuning Protocol Prioritization 2-8
Monitoring Statistics 2-8
Percent of Bandwidth 2-9
Queue Depth 2-10
Latency 2-12
Enabling Protocol Prioritization 2-12
Editing Protocol Prioritization Parameters 2-15
Enabling or Disabling Prioritization 2-18
Setting the High Queue Size 2-18
Setting the Normal Queue Size 2-18
Setting the Low Queue Size 2-18

Setting the Max High Queue Latency 2-19
Clearing the High-Water Mark 2-19
Selecting the Prioritization Algorithm Type 2-19
Setting the High Queue Percent Bandwidth 2-20
Setting the Normal Queue Percent Bandwidth 2-20
Setting the Low Queue Percent Bandwidth 2-21
Enabling or Disabling the Low-Priority Queue Discard Eligible Bit 2-21
Enabling or Disabling the Normal-Priority Queue Discard Eligible Bit 2-21

Chapter 3
Inbound Traffic Filter Criteria and Actions

Transparent Bridge Criteria and Actions 3-2
Predefined Transparent Bridge Criteria 3-3
User-Defined Transparent Bridge Criteria 3-4
Transparent Bridge Actions 3-4
Source Routing Bridge Criteria and Actions 3-5
Predefined Source Routing Criteria 3-5
Specifying a SRB Criterion Range 3-5
User-Defined Source Routing Criteria 3-6
Source Routing Actions 3-6
DECnet Phase IV Criteria and Actions 3-7
Predefined DECnet Criteria 3-7
User-Defined DECnet Criteria 3-7
DECnet Actions 3-7
DLSw Criteria and Actions 3-8
Predefined DLSw Criteria 3-8
User-Defined DLSw Criteria 3-8
DLSw Actions 3-8
IP Criteria and Actions 3-9
Predefined IP Criteria 3-9
User-Defined IP Criteria 3-9
IP Actions 3-10
IPX Criteria and Actions 3-11
Predefined IPX Criteria 3-11
User-Defined IPX Criteria 3-11
IPX Actions 3-11

LLC2 Criteria and Actions 3-12
Predefined LLC2 Criteria 3-12
User-Defined LLC2 Criteria 3-12
LLC2 Actions 3-12
OSI Criteria and Actions 3-13
Predefined OSI Criteria 3-13
User-Defined OSI Criteria 3-13
OSI Actions 3-13
VINES Criteria and Actions 3-14
Predefined VINES Criteria 3-14
User-Defined VINES Criteria 3-14
VINES Actions 3-14
XNS Criteria and Actions 3-15
Predefined XNS Criteria 3-15
User-Defined XNS Criteria 3-15
XNS Actions 3-15

Chapter 4
Outbound Traffic Filter Criteria and Actions

Predefined Criteria 4-2
Predefined Data Link Criteria 4-2
Predefined IP Criteria 4-4
Specifying Criteria Common to IP and Data Link Headers 4-5
Reference Points for User-Defined Criteria 4-6
Data Link Reference Points 4-6
IP Reference Points 4-8
Actions for Outbound Traffic Filters 4-9
Filtering Actions 4-9
Protocol Prioritization Actions 4-9
Dial-On-Demand Actions 4-10

Chapter 5
Specifying Common Criterion Ranges

Specifying MAC Address Ranges 5-2
Source Routing Bridge Source MAC Addresses 5-2
Source Routing Bridge Functional MAC Addresses 5-3

Specifying VINES Address Ranges 5-3
Specifying Source and Destination SAP Code Ranges 5-4
Specifying Frame Relay NLPID Range Values 5-5
Specifying PPP Protocol ID Range Values 5-5
Specifying TCP and UDP Port Range Values 5-5
Specifying Ethernet Type Range Values 5-7
Specifying IP Codes 5-10

Chapter 6
Applying Inbound Traffic Filters

Working with Inbound Traffic Filters 6-1
Displaying the Inbound Traffic Filters Window 6-2
Displaying the DLSw Inbound Traffic Filters Window 6-3
Preparing Filter Templates 6-4
Creating a New Template 6-5
Customizing Templates 6-12
Copying a Template 6-12
Editing a Template 6-13
Creating an Inbound Filter 6-15
Editing an Inbound Filter 6-17
Specifying User-Defined Criteria 6-20
Changing Filter Precedence 6-22
Enabling or Disabling an Inbound Filter 6-24
Deleting an Inbound Filter 6-26

Chapter 7
Applying Outbound Traffic Filters

Working with Outbound Traffic Filters 7-1
Displaying the Priority/Outbound Filters Window 7-2
Preparing Filter Templates 7-3
Creating a New Template 7-4
Specifying Prioritization Length 7-10
Customizing Templates 7-11
Copying a Template 7-11
Editing a Template 7-12
Creating an Outbound Filter 7-15

Editing an Outbound Filter 7-17
Changing Filter Precedence 7-20
Enabling or Disabling an Outbound Filter 7-22
Deleting an Outbound Filter 7-23

Appendix A
Site Manager Protocol Prioritization Parameters

Priority Interface Parameter Descriptions A-1
Prioritization Length Parameters A-7

Appendix B
Examples and Implementation Notes

Implementation Notes B-1
Filtering Outbound Frame Relay Traffic B-1
Filtering Over a Dial Backup Line B-2
Using a Drop-All Filter as a Firewall B-2
Inbound Traffic Filter Examples B-3
Creating an Inbound Traffic Filter Template (Predefined Criteria) B-4
Creating an Inbound Traffic Filter Template (User-Defined Criteria) B-5
Applying the Traffic Filter Template B-8
Protocol Prioritization Examples B-8

Index

Figures

Figure 2-1. Protocol Prioritization Dequeuing 2-3
Figure 2-2. Bandwidth Allocation Dequeuing Algorithm 2-5
Figure 2-3. Strict Dequeuing Algorithm 2-7
Figure 2-4. Priority Queue Statistics for the Queue Depth Example 2-11
Figure 2-5. Reconfigured Priority Queue Statistics for the Queue Depth Example 2-11
Figure 2-6. Circuit Definition Window 2-13
Figure 2-7. Selecting Protocol Priority from the Select Protocols List 2-14
Figure 2-8. Selecting the Edit Protocol Priority Interface Window 2-15
Figure 2-9. Edit Protocol Priority Interface Window (First Screen) 2-16
Figure 2-10. Edit Protocol Priority Interface Window (Scrolled Screen) 2-17
Figure 3-1. Header Reference Fields of Transparent Bridge Encapsulation Methods 3-2
Figure 4-1. Predefined Data Link Outbound Filter Criteria 4-3
Figure 4-2. Predefined IP Outbound Filter Criteria 4-5
Figure 4-3. Data Link Reference Points in a Source Routing Packet Bridged over Bay Networks Proprietary Frame Relay 4-7
Figure 4-4. Data Link Reference Points in an IEEE 802.2 LLC Header 4-7
Figure 4-5. IP Reference Points in a PPP Packet with IP Encapsulated Source Routing 4-8
Figure 6-1. Circuit List Window 6-2
Figure 6-2. Selecting the Inbound Traffic Filters Menu (Bridge Example) 6-3
Figure 6-3. Selecting the DLSw Inbound Traffic Filters Window 6-4
Figure 6-4. Inbound Traffic Filters Window 6-5
Figure 6-5. Filter Template Management Window 6-6
Figure 6-6. Create Template Window 6-7
Figure 6-7. Selecting a Filter Criterion 6-8
Figure 6-8. Add Range Window 6-9
Figure 6-9. Create Template Window with Criteria and Range Added 6-10
Figure 6-10. Actions List with New Action 6-11

Figure 6-11. Copy Filter Template Window 6-12
Figure 6-12. Create Filter Window 6-15
Figure 6-13. New Filter Listed in the Filters Window Scroll Box 6-16
Figure 6-14. Edit Filters Window 6-18
Figure 6-15. Add User-Defined Field Window 6-20
Figure 6-16. User-Defined Criteria 6-21
Figure 6-17. Traffic Filters List (in Order Created) 6-22
Figure 6-18. Change Precedence Window 6-23
Figure 6-19. Traffic Filters List (Reordered Precedence) 6-24
Figure 6-20. Traffic Filters Window 6-25
Figure 7-1. Selecting the Priority/Outbound Filters Window 7-3
Figure 7-2. Priority/Outbound Filters Window 7-4
Figure 7-3. Filter Template Management Window 7-5
Figure 7-4. Create Priority/Outbound Template Window 7-6
Figure 7-5. Selecting Outbound Traffic Filter Criteria 7-7
Figure 7-6. Add Range Window 7-8
Figure 7-7. Create Priority/Outbound Template Window with Criteria and Actions 7-9
Figure 7-8. Prioritization Length Window 7-10
Figure 7-9. Copy Filter Template Window 7-12
Figure 7-10. Edit Priority/Outbound Template Window 7-13
Figure 7-11. Priority/Outbound Filters Window 7-15
Figure 7-12. Create Filter Window 7-16
Figure 7-13. Edit Priority/Outbound Filters Window 7-18
Figure 7-14. Sample List of Outbound Filters 7-20
Figure 7-15. Change Precedence Window 7-21
Figure 7-16. Example of Outbound Filter Order Change 7-22

Tables

Table 1-1. Predefined Inbound Traffic Filter Criteria 1-9
Table 1-2. Predefined Outbound Traffic Filter Criteria 1-11
Table 1-3. Summary of Traffic Filter Support 1-17
Table 3-1. Bridge Encapsulation Support for Physical Media Types 3-3
Table 3-2. Predefined Criteria for Transparent Bridge Encapsulations 3-3
Table 3-3. Predefined Criteria for Source Routing Bridge 3-5
Table 3-4. Predefined Criteria for DECnet Inbound Traffic Filters 3-7
Table 3-5. Predefined Criteria for DLSw Inbound Traffic Filters 3-8
Table 3-6. Predefined Criteria for IP Inbound Traffic Filters 3-9
Table 3-7. Predefined Criteria for IPX Inbound Traffic Filters 3-11
Table 3-8. Predefined Criteria for LLC2 Inbound Traffic Filters 3-12
Table 3-9. Predefined Criteria for OSI Inbound Traffic Filters 3-13
Table 3-10. Predefined Criteria for VINES Inbound Traffic Filters 3-14
Table 3-11. Predefined Criteria for XNS Inbound Traffic Filters 3-15
Table 4-1. Predefined Data Link Outbound Filter Criteria 4-2
Table 4-2. Predefined IP Outbound Filter Criteria 4-4
Table 4-3. Data Link Reference Points 4-6
Table 4-4. IP Reference Points 4-8
Table 5-1. Format for Specifying Source-Routing MAC Addresses 5-2
Table 5-2. Functional MAC Addresses 5-3
Table 5-3. SAP Codes 5-4
Table 5-4. Frame Relay NLPID Values 5-5
Table 5-5. PPP Protocol ID Values 5-5
Table 5-6. Source and Destination TCP Port Values 5-5
Table 5-7. Source and Destination UDP Port Values 5-6
Table 5-8. Ethernet Type Codes 5-7
Table 5-9. IP Type Codes 5-10
Table 6-1. Using the Edit Filter Template Window 6-14
Table 6-2. Using the Edit Filters Window 6-19

Table 7-1. Using the Edit Priority/Outbound Filter Template Window 7-14
Table 7-2. Using the Edit Priority/Outbound Filters Window 7-19
Table B-1. Predefined Criteria, Ranges, and Actions for Example Inbound Traffic Filters B-5
Table B-2. User-Defined Criteria and Ranges for Example Inbound Traffic Filters .. B-7
Table B-3. Example Criteria, Ranges, and Actions for Protocol Prioritization B-10

About This Guide

Read this guide to learn how to customize Bay Networks router software to filter and prioritize traffic. *Configuring Traffic Filters and Protocol Prioritization* offers

- An overview of traffic filters (Chapter 1)
- An overview of protocol prioritization and instructions for customizing protocol prioritization configuration parameters (Chapter 2)
- Protocol-specific reference information on inbound traffic filter criteria and actions (Chapter 3)
- Protocol-specific reference information on outbound traffic filter criteria and actions (Chapter 4)
- Information on specifying inbound and outbound criteria ranges (Chapter 5)
- Instructions on using the Configuration Manager to create inbound traffic filters (Chapter 6)
- Instructions on using the Configuration Manager to create outbound traffic filters (Chapter 7)
- Site Manager parameter descriptions (Appendix A)
- Configuration examples and implementation notes (Appendix B)

Before You Begin

Before using this guide, make sure that the router is running the latest version of Bay Networks Site Manager and router software. For instructions, refer to *Upgrading Routers from Version 7–10.xx to Version 11.0*.

For a new router:

1. Install the router.

   Refer to the installation manual that came with your router.

2. Connect the router to the network and create a configuration file.

   For instructions, refer to one of the following manuals:

   - *Quick-Starting Routers*
   - *Connecting ASN Routers to a Network*
   - *Connecting BayStack AN and ANH Systems to a Network*

Conventions

bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.
`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu.
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is
	show at routes | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

ANSI	American National Standards Institute
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
DE	Discard Eligible
DLC	Data Link Control
DLSw	data link switching
DSAP	Destination Service Access Point
FTP	file transfer protocol
ICMP	Internet Control Message Protocol
HDLC	high-level data link control
IP	Internet Protocol
IPX	Internet Package Exchange
LAT	Local Area Transport
LLC	logical link control
LLM	LAN Network Manager
MAC	media access control
MSB	most significant bit
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (Interior Gateway Protocol)
OSPF/BGP	Open Shortest Path First/Border Gateway Protocol
PPP	Point-to-Point Protocol
RIF	routing information field
RIP	Routing Information Protocol
SAP	Service Access Point
SDLC	Synchronous Data Link Control
SMDS	switched multimegabit data service
SNA	Systems Network Architecture (IBM)
SNAP	Subnetwork Access Protocol
SRB	source routing bridge
SSAP	Source Service Access Point
TCP	Transmission Control Protocol

TELNET	Telecommunication Network
UDP	User Datagram Protocol
VINES	Virtual Networking System (Banyan)
XNS	Xerox Network System

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from the Bay Networks Press™ at the following telephone or fax numbers:

- Telephone - U.S./Canada 1-888-4BAYPRESS
- Telephone - International 1-510-490-4752
- Fax 1-510-498-2609

You can also use these numbers to request a free catalog of Bay Networks Press product publications.

Technical Support and Online Services

To ensure comprehensive network support to our customers and partners worldwide, Bay Networks Customer Service has Technical Response Centers in key locations around the globe:

- Billerica, Massachusetts
- Santa Clara, California
- Sydney, Australia
- Tokyo, Japan
- Valbonne, France

The Technical Response Centers are connected via a redundant Frame Relay Network to a Common Problem Resolution system, enabling them to transmit and share information, and to provide live, around-the-clock support 365 days a year.

Bay Networks Information Services complement the Bay Networks Service program portfolio by giving customers and partners access to the most current technical and support information through a choice of access/retrieval means. These include the World Wide Web, CompuServe, Support Source CD, Customer Support FTP, and InfoFACTS document fax service.

Bay Networks Customer Service

If you purchased your Bay Networks product from a distributor or authorized reseller, contact that distributor's or reseller's technical support staff for assistance with installation, configuration, troubleshooting, or integration issues.

Customers can also purchase direct support from Bay Networks through a variety of service programs. As part of our PhonePlus™ program, Bay Networks Service sets the industry standard, with 24-hour, 7-days-a-week telephone support available worldwide at no extra cost. Our complete range of contract and noncontract services also includes equipment staging and integration, installation support, on-site services, and replacement parts delivery -- within approximately 4 hours.

To purchase any of the Bay Networks support programs, or if you have questions on program features, use the following numbers:

Region	Telephone Number	Fax Number
United States and Canada	1-800-2LANWAN; enter Express Routing Code (ERC) 290 when prompted (508) 436-8880 (direct)	(508) 670-8766
Europe	(33) 92-968-300	(33) 92-968-301
Asia/Pacific Region	(612) 9927-8800	(612) 9927-8811
Latin America	(407) 997-1713	(407) 997-1714

In addition, you can receive information on support programs from your local Bay Networks field sales office, or purchase Bay Networks support directly from your authorized partner.

Bay Networks Information Services

Bay Networks Information Services provide up-to-date support information as a first-line resource for network administration, expansion, and maintenance. This information is available from a variety of sources.

World Wide Web

The Bay Networks Customer Support Web Server offers a diverse library of technical documents, software agents, and other important technical information to Bay Networks customers and partners.

A special benefit for contracted customers and resellers is the ability to access the Web Server to perform Case Management. This feature enables your support staff to interact directly with the network experts in our worldwide Technical Response Centers. A registered contact with a valid Site ID can

- View a listing of support cases and determine the current status of any open case. Case history data includes severity designation, and telephone, e-mail, or other logs associated with the case.
- Customize the listing of cases according to a variety of criteria, including date, severity, status, and case ID.
- Log notes to existing open cases.
- Create new cases for rapid, efficient handling of noncritical network situations.
- Communicate directly via e-mail with the specific technical resources assigned to your case.

The Bay Networks URL is *http://www.baynetworks.com*. Customer Service is a menu item on that home page.

Customer Service FTP

Accessible via URL *ftp://support.baynetworks.com* (134.177.3.26), this site combines and organizes support files and documentation from across the Bay Networks product suite, including switching products from our Centillion™ and Xylogics® business units. Central management and sponsorship of this FTP site lets you quickly locate information on any of your Bay Networks products.

Support Source CD

This CD-ROM -- sent quarterly to all contracted customers -- is a complete Bay Networks Service troubleshooting knowledge database with an intelligent text search engine.

The Support Source CD contains extracts from our problem-tracking database; information from the Bay Networks Forum on CompuServe; comprehensive technical documentation, such as Customer Support Bulletins, Release Notes, software patches and fixes; and complete information on all Bay Networks Service programs.

You can run a single version on Macintosh Windows 3.1, Windows 95, Windows NT, DOS, or UNIX computing platforms. A Web links feature enables you to go directly from the CD to various Bay Networks Web pages.

CompuServe

For assistance with noncritical network support issues, Bay Networks Information Services maintain an active forum on CompuServe, a global bulletin-board system. This forum provides file services, technology conferences, and a message section to get assistance from other users.

The message section is monitored by Bay Networks engineers, who provide assistance wherever possible. Customers and resellers holding Bay Networks service contracts also have access to special libraries for advanced levels of support documentation and software. To take advantage of CompuServe's recently enhanced menu options, the Bay Networks Forum has been re-engineered to allow links to our Web sites and FTP sites.

We recommend the use of CompuServe Information Manager software to access these Bay Networks Information Services resources. To open an account and receive a local dial-up number in the United States, call CompuServe at 1-800-524-3388. Outside the United States, call 1-614-529-1349, or your nearest CompuServe office. Ask for Representative No. 591. When you are on line with your CompuServe account, you can reach us with the command **GO BAYNET**.

InfoFACTS

InfoFACTS is the Bay Networks free 24-hour fax-on-demand service. This automated system has libraries of technical and product documents designed to help you manage and troubleshoot your Bay Networks products. The system responds to a fax from the caller or to a third party within minutes of being accessed.

To use InfoFACTS in the United States or Canada, call toll-free 1-800-786-3228. Outside North America, toll calls can be made to 1-408-764-1002. In Europe, toll-free numbers are also available for contacting both InfoFACTS and CompuServe. Please check our Web page for the listing in your country.

How to Get Help

Use the following numbers to reach your Bay Networks Technical Response Center:

Technical Response Center	Telephone Number	Fax Number
Billerica, MA	1-800-2LANWAN	(508) 670-8765
Santa Clara, CA	1-800-2LANWAN	(408) 764-1188
Valbonne, France	(33) 92-968-968	(33) 92-966-998
Sydney, Australia	(612) 9927-8800	(612) 9927-8811
Tokyo, Japan	(81) 3-5402-0180	(81) 3-5402-0173

Chapter 1
Using Traffic Filters

To help you understand and plan for traffic filter configurations on Bay Networks routers, this chapter defines and describes the following concepts:

- What Are Traffic Filters?
- What Is Protocol Prioritization?
- What Do Traffic Filters Do?
- Filtering Strategies
- Components of Traffic Filters
- Using Filter Templates
- Traffic Filter Summary

What Are Traffic Filters?

Traffic filters are router files that instruct an interface to selectively handle specified network traffic (packets, frames, or datagrams). Using traffic filters, you can block, forward, log, or prioritize certain traffic on an interface. You determine which packets receive special handling based on information fields within the packet headers.

There are two types of traffic filters:

- *Inbound traffic filters*, which act on packets coming in to the router
- *Outbound traffic filters*, which act on packets that the router is forwarding

Note: Be careful not to confuse traffic filters with other router filters such as route filters, which force filtered protocol traffic to take particular routes.

You can create traffic filters on the following interfaces:

- Ethernet (10Base-T and 100Base-T)
- FDDI
- HSSI
- MCE1
- MCT1
- Synchronous
- Token Ring

You can apply multiple traffic filters to a single interface. When more than one filter applies to a packet, the order of filters determines the final filtering result.

Inbound Traffic Filters

Inbound traffic filters act on packets coming in a particular router interface. When you configure inbound filters, you specify a set of conditions that apply to the traffic of a particular bridging or routing protocol. The Configuration Manager supports inbound traffic filters for the following protocols:

- Transparent Bridge (four encapsulation methods: Ethernet, 802.2 LLC, 802.2 LLC with SNAP, and Novell Proprietary)
- Native Source Routing
- IP
- IPX
- XNS
- OSI
- DECnet Phase IV
- VINES
- DLSw
- LLC2 (APPN and LNM)

Most sites use inbound traffic filters primarily for security, to restrict access to particular source locations on a network or to certain types of data.

Chapter 3 provides protocol-specific information for designing inbound filters. Chapter 6 explains how to use the Configuration Manager to apply inbound filters.

Outbound Traffic Filters

Outbound traffic filters act on packets that the router forwards to a local or wide-area network through a particular interface.

Note: In some configurations, implementing outbound traffic filters for LAN protocols may cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, we suggest that you monitor the throughput performance after configuring outbound LAN filters. If you notice an unacceptable performance degradation, it may be best to use inbound traffic filters to accomplish the filtering goal.

Outbound traffic filters are not based on a routing protocol, as are inbound traffic filters. When you configure outbound traffic filters, you specify a set of conditions that apply to the packet's

- Data Link header
- IP header

To use outbound traffic filters, you select Protocol Priority as one of the configured protocols on an interface. Protocol Priority is enabled by default on circuits configured with Frame Relay or PPP. Otherwise, you must enable Protocol Priority the first time you configure outbound traffic filters on an interface.

Chapter 4 provides information for designing outbound filters. Chapter 7 explains how to use the Configuration Manager to enable Protocol Priority and apply outbound filters.

What Is Protocol Prioritization?

As a router operates, network traffic from a variety of sources converges at each WAN interface. Without protocol prioritization, the router transmits packets in a first-in, first-out (FIFO) order. By implementing protocol prioritization, you instruct the router to use a different transmit order for specified ranges of packets.

With protocol prioritization enabled, the router sorts the WAN traffic on an individual interface into three delivery queues of varying precedence (high, normal, and low priority), called *priority queues*. The router then uses a dequeuing algorithm to drain the priority queues and transmit traffic.

Protocol prioritization is an outbound filter mechanism, because

- You use outbound traffic filters to specify whether and how traffic gets sorted into priority queues.
- Priority queues affect the sequence in which data leaves an interface; they do not affect traffic as it enters the router.

Outbound filters that include a protocol prioritization action are sometimes called *priority filters*. You can apply priority filters to MCE1, MCT1, and synchronous interfaces

Note: Outbound traffic filters on LAN interfaces do not support protocol prioritization.

Refer to Chapter 2 to learn more about priority queuing and dequeuing.

DLSw Prioritization Filters

DLSw prioritization allows you to prioritize traffic *within DLSw*, based on predefined or user-defined fields at the TCP level. Examples of DLSw prioritization criteria include

- Source and destination SAP; you can use this to assign NetBIOS traffic (SAP 0xF0) to a lower priority than SNA traffic
- Source and destination MAC address; you can use this to provide host bound traffic preference over other traffic
- Any field in the SNA transmission header (TH) and response/request header (RH); you can use this to provide class of service (COS) priority preference

You can also prioritize traffic based on any user-defined values within the headers and data packets.

For detailed information about DLSw prioritization filters, refer to *Configuring DLSw Services*.

What Do Traffic Filters Do?

You use inbound traffic filters primarily for security, to deflect certain traffic from destination nodes in your network. You use outbound filters primarily to ensure timely delivery of critical data.

Ensure Consistent Service

When a router treats all packets equally, there is no way to ensure consistent network services to users who are working interactively. Bulk transfer applications use too much of the available bandwidth and slow down interactive response times. These problems are especially visible on low-speed WAN links.

Reduce Network Congestion

Both inbound and outbound traffic filters reduce network congestion by minimizing the flow of unnecessary traffic over LAN and WAN segments.

Prioritize Important Traffic

You can use protocol prioritization to expedite traffic coming from a particular source or going to a certain destination.

Reduce Loss of Critical Data

You can improve application response time and eliminate session timeouts by implementing protocol prioritization.

Enhance Security

Inbound and outbound traffic filters are an integral part of a comprehensive network security strategy. You can control access to individual stations, networks, and network resources through predefined or user-defined filter criteria. You can use outbound filters to drop completely (*clip*) any traffic you do not want leaving the local network.

Filtering Strategies

This section suggests some ways you might use traffic filters in a network. Refer to Appendix B for specific examples.

Drop or Accept Certain Traffic

To accept only specified traffic and drop other packets, configure accept filters. To accept most traffic and drop only specified packets, configure filters only for the traffic you want to drop.

Note: Drop filters usually perform more efficiently than accept filters.

For example, to prevent all NetBIOS traffic from entering a particular LAN segment, you can create an inbound traffic filter to drop all packets with a Destination or Source SAP code of F0.

Build a Firewall

If your filtering strategy involves blocking most traffic and accepting only specified packets (a *firewall*) begin with a drop-all filter on the interface. That means you choose a filter criterion that appears in *every* packet of the protocol you are filtering (for example, a MAC address). Then, add more specific, higher-precedence Accept and Drop filters to achieve the desired result on that interface. Refer to “Using a Drop-All Filter as a Firewall” in Appendix B for more information.

Direct Certain Traffic

You can create traffic filters that affect only a particular protocol’s traffic. For example, you can forward all IP traffic to a next-hop address. You can also create bridge traffic filters that affect certain locations on the network. For example, if you want all traffic from a node with a particular MAC address (perhaps an application server) to take precedence over other traffic, you can use protocol prioritization to assign a high priority to any traffic with that source address.

Combine Filters

You can apply as many as 31 inbound and 31 outbound traffic filters per protocol.

As you add filters to an interface, the Configuration Manager numbers them chronologically (Filter No. 1, Filter No. 2, Filter No. 3, and so on). The filter rule number determines the filter's *precedence.* Lower numbers have higher precedence; Filter No. 1 has the highest precedence. If a packet matches 2 filters, the filter with the highest precedence (lowest number) applies.

You can reorder filters after creating them to determine the precedence of individual filters. Refer to the "Changing Filter Precedence" section in Chapter 6 (inbound traffic filters) or Chapter 7 (outbound traffic filters).

Components of Traffic Filters

Site Manager creates both inbound and outbound traffic filters from template files that contain filtering information. Traffic filter templates consist of three components:

- *Criteria*
  The part of each incoming packet, frame, or datagram header to be examined
- *Ranges*
  Numeric values (usually addresses) to be compared with the contents of examined packets
- *Actions*
  What happens to packets that match the criteria and ranges specified in a filter

To create a traffic filter, you apply a filter template to a particular router interface. Table 1-3 (at the end of this chapter) summarizes the inbound and outbound filter criteria and actions supported on specific interfaces.

Criteria

A filter criterion is the part of a packet, frame, or datagram header to be examined. You can logically break down any packet into at least three components:

- The data link control (DLC) header. Examples of DLC header types are
  - -- Token Ring (802.5)
  - -- Ethernet V.2 and IEEE 802.3
  - -- FDDI
  - -- PPP and Bay Networks Standard
  - -- Frame Relay
- The upper-level protocol header. Examples of protocol header types include:
  - -- IP and TCP
  - -- Source route bridge
  - -- DLSw
- User data

A traffic filter criterion is defined by a byte length and an offset from common bit patterns (*reference points*) within the DLC or protocol header. The criterion includes the *length* of the filtered pattern and an *offset* from the known reference point. The traffic filter uses this information to locate which part of a packet to examine.

For all bridge traffic, predefined criteria are part of the DLC header. For routed traffic, a predefined criterion can be part of the DLC header or part of an upper-level network protocol header.

Inbound traffic filter criteria use reference points in the upper-level protocol header. You select inbound criteria based on the protocol of the incoming traffic. Outbound traffic filters use reference points in only the IP or DLSw protocol headers. You select outbound criteria based on the WAN protocol configured on the interface (Bridge, Source Routing, PPP, or Frame Relay).

Predefined and User-Defined Criteria

The Configuration Manager provides a selection of default filter criteria (*predefined criteria*) for both inbound and outbound traffic filters. Predefined criteria consist of predefined offsets and lengths from common reference points.

Instead of using a predefined filter criterion, you can define a criterion by specifying the length and offset from a supported reference point (*user-defined criteria*).

One filter can employ multiple criteria, including a combination of predefined and user-defined criterion, to fit a site's traffic patterns.

Predefined Criteria

Table 1-2 summarizes the predefined inbound traffic filter criteria for supported protocols.

Table 1-1. Predefined Inbound Traffic Filter Criteria

Protocol	Predefined Criteria
Transparent Bridge (Four Data Link encapsulation methods: Ethernet, 802.2 LLC, Novell Proprietary, 802.2 LLC with SNAP)	MAC Address (Source or Destination) Ethernet type Novell 802.2 LLC Length 802.2 LLC DSAP 802.2 LLC SSAP 802.2 LLC Control 802.2 SNAP Length 802.2 SNAP Protocol ID 802.2 SNAP Ethernet Type
Source Route Bridge (Native only; IP-encapsulated SRB is not supported)	MAC Address (Source or Destination) DSAP SSAP NetBIOS Name (Source or Destination)
DECnet Phase IV	Area (Source or Destination) Node (Source or Destination)
DLSw	MAC Address (Source or Destination) DSAP SSAP

(continued)

Table 1-1. Predefined Inbound Traffic Filter Criteria *(continued)*

Protocol	Predefined Criteria
IP	Type of Service IP Address (Source and/or Destination) UDP port (Source and/or Destination) TCP port (Source and/or Destination) Established TCP protocols Protocol Type
IPX	Network (Source or Destination) Host Address (Source or Destination) Socket (Source or Destination)
OSI	OSI Area (Source or Destination) System ID (Source or Destination)
LLC2	MAC Address (Source or Destination) DSAP SSAP
VINES	Protocol Type VINES Address (Source or Destination)
XNS	Network (Source or Destination) Address (Source or Destination) Socket (Source or Destination)

Table 1-2 summarizes the predefined outbound traffic filter criteria for DLC and IP headers.

Note: See *Configuring DLSw Services* for information about criteria for outbound traffic filters based on the DLSw header.

Table 1-2. Predefined Outbound Traffic Filter Criteria

Header	Traffic Type	Predefined Outbound Filter Criteria
Data Link Control Header	Transparent Bridge (Data Link Type)	MAC Address (Source or Destination) Ethernet Type Novell 802.2 Length 802.2 DSAP 802.2 SSAP 802.2 Control 802.2 SNAP Length 802.2 SNAP Protocol ID 802.2 SNAP Ethernet Type
	Source Routing	SSAP DSAP
	PPP	Protocol ID
	Frame Relay	2-byte DLCI 3-byte DLCI 4-byte DLCI NLPID Ethernet Type
IP Header	IP	Type of Service Priority_IP Address (Source and/or Destination) UDP port (Source and/or Destination) TCP port (Source and/or Destination) Established TCP Protocol Type
	Source Routing	SSAP Destination Address Source Address
	PPP	Protocol ID
	Frame Relay	2-byte DLCI 3-byte DLCI 4-byte DLCI NLPID

User-Defined Criteria

To apply customized criteria that use fields that are not represented in a protocol's predefined criteria, you can create a user-defined criterion. You specify its location within the packet header in terms of three parameters:

- Reference point

  Specifies a predefined, known bit position within the packet header

- Offset

  Specifies the beginning position of the filtered bit pattern in relation to the reference point (measured in bits)

- Length

  Specifies the total bit length of the filtered pattern

Ranges

For each traffic filter criterion, you also specify the valid *range*, a series of target values appropriate to the criterion. For most criteria, you specify an address range. There must be at least one target value per criterion. The range can be just one value, or it can be a set of values.

You enter a minimum and a maximum value to specify the range. (For a range of only one value, you enter only the minimum value; the Configuration Manager automatically uses that value for both the minimum and maximum.)

For example, if the filter criteria is MAC Source Address, you must specify *which* addresses you want the filter to examine. If you specify 0x0000A2000001 as the minimum range value and 0x0000A2000003 as the maximum range value, the router checks for packets with a MAC source address between 0x0000A2000001 and 0x0000A2000003, inclusive.

Note: Chapter 5 lists valid range values for common traffic filter criteria and explains how to specify some common address ranges.

Actions

The filter *action* determines what happens to packets that match a filter criterion's ranges. Site Manager supports

- Filtering Actions
- Prioritizing Actions
- Dial Service Actions

Note: In addition to the traffic filter actions described in this section, there are additional, protocol-specific actions for Bridge, IP, and DLSw inbound traffic filters, described in Chapter 3.

Filtering actions are common to all traffic filters. Prioritizing and Dial Service actions are available only for outbound traffic filters on WAN interfaces.

Except the Log action, traffic filter actions are mutually exclusive; you can only apply one action per filter.

Filtering Actions

You can apply the following actions to any traffic filter:

- Accept

  The router processes any packet that matches the filter criteria and ranges.

- Drop

  The router does not route any packet that matches the filter criteria and ranges.

- Log

  For every packet that matches the filter criteria and ranges, the router sends an entry to the system Events log. You can specify the Log action in combination with other actions.

Note: Specify the Log action only to record abnormal events; otherwise, the Events log will fill up with filtering messages, leaving no room for critical log messages.

Prioritizing Actions

Outbound traffic filters for WAN protocols include the following actions for directing matching traffic into protocol prioritization queues:

- High

  Packets that match the filter criteria and ranges are processed in the high queue.

- Low

  Packets that match the filter criteria and ranges are processed in the low queue.

- Length

  For packets that match the filter criteria, the packet length determines the priority queue into which it is placed.

Note: Site Manager does not support prioritizing actions on LAN interfaces.

See "What Is Protocol Prioritization?" earlier in this chapter for a brief overview. See Chapter 2 for detailed information about the protocol prioritization process.

Dial Service Actions

Outbound traffic filters for interfaces configured as dialup lines include the following actions:

- No Call

  Packets that match the filter criteria and ranges are dropped and do not initiate a dial connection.

- No Reset

  Packets that match the filter criteria and ranges are processed but do not reset the inactivity timer.

Note: Although No Call and No Reset are available when creating outbound traffic filters on any interface, these actions are useful only on dial interfaces such as synchronous modem lines or an MCT1 interfaces configured with ISDN PRI.

By default, packets transmitted on dial-on-demand lines always trigger the router to establish a connection. You can use the dial service actions to configure outbound traffic filters that specify or reduce the type of traffic to initiate dial connections.

For example, dial optimized routing is a method of exchanging IP RIP and IPX RIP/SAP routing updates only when the router activiates connections for *data* transmissions. This reduction in update-only traffic limits unecessary connections and reduced line costs.

See *Configuring Dial Services* for information about dial services such as dial optimized routing.

Using Filter Templates

When you create traffic filters, it is important to understand the difference between a traffic filter template and an actual traffic filter. A traffic filter *template* is a reusable, predefined specification for a traffic filter. Each template contains a complete filter specification (criterion, range, and action) for one protocol, but is not associated with a specific interface or circuit.

You create an actual traffic filter when you use the Configuration Manager to apply (save) a traffic filter template to a configured router interface. You can apply a single template to as many interfaces as you want, thus creating multiple filters for that protocol.

When you want to add a filter to an interface, you have several options:

- If there is a template that contains the exact filtering instructions that you want for this interface, apply that template to this interface.
- If there is a template that contains filtering instructions similar to what you want, copy, rename, and edit the template. Then apply the new template to the appropriate interface.
- If there is no template containing filtering instructions similar to what you want for this interface, you must create a template from scratch. Then apply the new template to the appropriate interface.
- If there is an existing filter on the interface that contains instructions similar to what you want, edit the existing filter directly and save it.

Creating a Template

You create traffic filter templates using protocol-specific windows within the Configuration Manager. You can create as many as 500 traffic filter templates for each interface.

Note: You can also edit or copy a template using a text editor. The Configuration Manager stores all templates for all protocols in a file called *template.flt*. In the Unix file system, the pathname is */usr/filters/template.flt*.

To create and use a filter template:

1. **Name the template.**

   It is a good idea to give each template a descriptive name. For example, if you are building a template that is going to instruct the interface to drop all DECnet Phase IV traffic with a Source Node value of 3, name it *dec_Snode_3*. Or, if you are building a template that is going to instruct the interface to queue all LAT traffic to the high priority queue, name the template something like *LAT_high.*

2. **Select a protocol-specific criterion, range, and action.**

   Select the criteria and address range or ranges for checking packets. Then select the action to impose on packets that match the specified criteria and ranges.

Note: Because you create filter templates on a per-protocol basis, you must become familiar with the specific criteria and actions used for filtering by each protocol before creating templates.

3. **Save the template file.**

4. **Apply the template to an interface to create a filter.**

   After you save the template file, you can apply that template to as many interfaces as you want. The template remains for future use unless you explicitly delete it.

For a detailed, step-by-step example of how to create a filter template, follow the procedure in Chapter 6 (for inbound filters) or Chapter 7 (for outbound filters).

Traffic Filter Summary

Table 1-3 summarizes the inbound and outbound traffic filter criteria and actions supported on specific interfaces.

Table 1-3. Summary of Traffic Filter Support

Network Interface	Protocol Criteria Supported		Filter Actions Supported	
	Inbound	**Outbound**	**Inbound**	**Outbound**
Ethernet (10Base-T or 100Base-T)	Transparent Bridge[1], DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, IP, Source Route Bridge	Accept, Drop, Log [3]	Accept, Drop, Log
FDDI	Transparent Bridge[2], DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, IP, Source Route Bridge	Accept, Drop, Log [3]	Accept, Drop, Log
Token Ring	Transparent Bridge[2], DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, IP, Source Route Bridge	Accept, Drop, Log [3]	Accept, Drop, Log
HSSI	Transparent Bridge[2], DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Accept, Drop, Log	Accept, Drop, Log [3]	Accept, Drop, Log
MCE1	Transparent Bridge, DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, Frame Relay, IP, PPP, Source Route Bridge	None	Accept, Drop, Log, High Queue, Low Queue, Length, No Call, No Reset
MCT1	Transparent Bridge, DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, Frame Relay, IP, PPP, Source Route Bridge	None	Accept, Drop, Log, High Queue, Low Queue, Length, No Call, No Reset
Synchronous	Transparent Bridge[1], DECnet IV, DLSw, IP, IPX, LLC2, OSI, Source Route, XNS, VINES	Transparent Bridge, Frame Relay, IP, PPP, Source Route Bridge	Accept, Drop, Log [3]	Accept, Drop, Log, High Queue, Low Queue, Length, No Call, No Reset

[1] Ethernet, 802.2 LLC, LLC with SNAP, and Novell encapsulations

[2] 802.2 LLC and LLC with SNAP encapsulations

[3] Plus additional actions for Bridge and IP filters

Chapter 2
Using Protocol Prioritization

This chapter describes the priority queuing (*protocol prioritization*) you can implement using outbound traffic filters. Site Manager supports protocol prioritization on synchronous, HSSI, MCE1, and MCT1 interfaces for the following WAN protocols:

- PPP (Point-to-Point Protocol)
- Standard (Bay Networks Standard PPP)
- Frame Relay

Note: You cannot implement protocol prioritization on LAN interfaces or protocols.

For information on DLSw prioritization, see the *Configuring DLSw Services* guide.

The first section of this chapter provides an overview of priority queues. Subsequent sections describe

- Tuning Protocol Prioritization
- Enabling Protocol Prioritization
- Editing Protocol Prioritization Parameters

For instructions on using the Configuration Manager to create outbound traffic filters, refer to Chapter 7.

About Priority Queues

Depending on how you configure protocol priority, the router queues each packet and holds them in one of three priority queues:

- High queue
- Normal queue
- Low queue

The router automatically queues packets that do not match a traffic filter to the normal priority queue.

The Dequeuing Process

After queuing packets, the router empties the priority queues by sending the traffic to the transmit queue. Generally, the router transmits higher priority traffic first. Other configured values in the protocol prioritization scheme also affect the transmission of traffic. Two of these configurable values are *queue depth* and line delay, or *latency*, described in the section“Tuning Protocol Prioritization.”

Protocol prioritization uses one of two dequeuing algorithms to send traffic to the transmit queue: the *Bandwidth Allocation Algorithm* or the *Strict Dequeuing Algorithm*.

By default, protocol prioritization uses the bandwidth allocation algorithm to send traffic to the transmit queue. This is because if the router uses the strict dequeuing algorithm and there is a great deal of high-priority traffic on the network, the normal- and low-priority traffic may never get transmitted.

You specify the active dequeuing algorithm as described in the section “Editing Protocol Prioritization Parameters” later in this chapter.

Figure 2-1 illustrates the dequeuing process, with default configuration values.

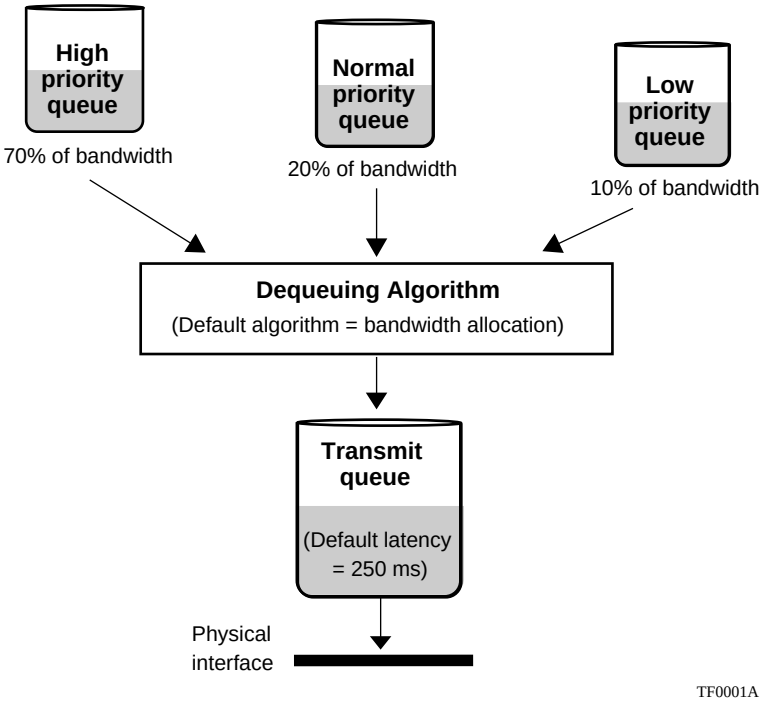

Figure 2-1. Protocol Prioritization Dequeuing

Bandwidth Allocation Algorithm

The bandwidth allocation algorithm uses a configurable percentage of bandwidth for each of the three priority queues to determine how to transmit queued traffic. The default configuration is

- HighQ -- 70% of bandwidth
- NormalQ -- 20% of bandwidth
- LowQ -- 10% of bandwidth

When the amount of traffic transmitted from a particular queue reaches the configured percentage, the next priority queue begins to transmit traffic.

The amount of actual data transmitted depends on the clock speed of the circuit. You can configure the clock speed on a synchronous interface by setting the External Clock Speed parameter in the Configuration Manager Edit Sync Parameters window. Refer to *Configuring Line Services*.

The bandwidth allocation algorithm works as follows:

1. **The transmit queue scans the high-priority queue.**

   If there is no traffic in the high-priority queue, the algorithm proceeds to Step 3.

2. **The router empties all packets from the high-priority queue, up to the configured bandwidth percentage, into the transmit queue and transmits them.**

   The default bandwidth percentage for high-priority traffic is 70 percent. If the actual bandwidth use is less than the limit, the router empties the high-priority queue and proceeds to the normal-priority queue.

3. **The transmit queue scans the normal-priority queue.**

   If there is no traffic in the normal-priority queue, the algorithm proceeds to Step 5.

4. **The router empties all packets from the normal-priority queue, up to the bandwidth percentage you have configured, into the transmit queue and transmits them.**

   The default bandwidth percentage for the normal-priority queue is 20 percent. If the actual bandwidth use is less than the limit, the router empties the normal-priority queue and proceeds to the next queue.

5. **The transmit queue scans the low-priority queue.**

   If there is no traffic in the low-priority queue, the algorithm starts again at Step 1.

6. **The router empties all packets from the low-priority queue, up to the bandwidth percentage you have configured, into the transmit queue and transmits them.**

   The default bandwidth percentage for the low-priority queue is 10 percent. If the actual bandwidth use is less than the limit, the router empties the low-priority queue.

7. **The algorithm starts again at Step 1.**

Figure 2-2 illustrates the algorithm for bandwidth allocation dequeuing.

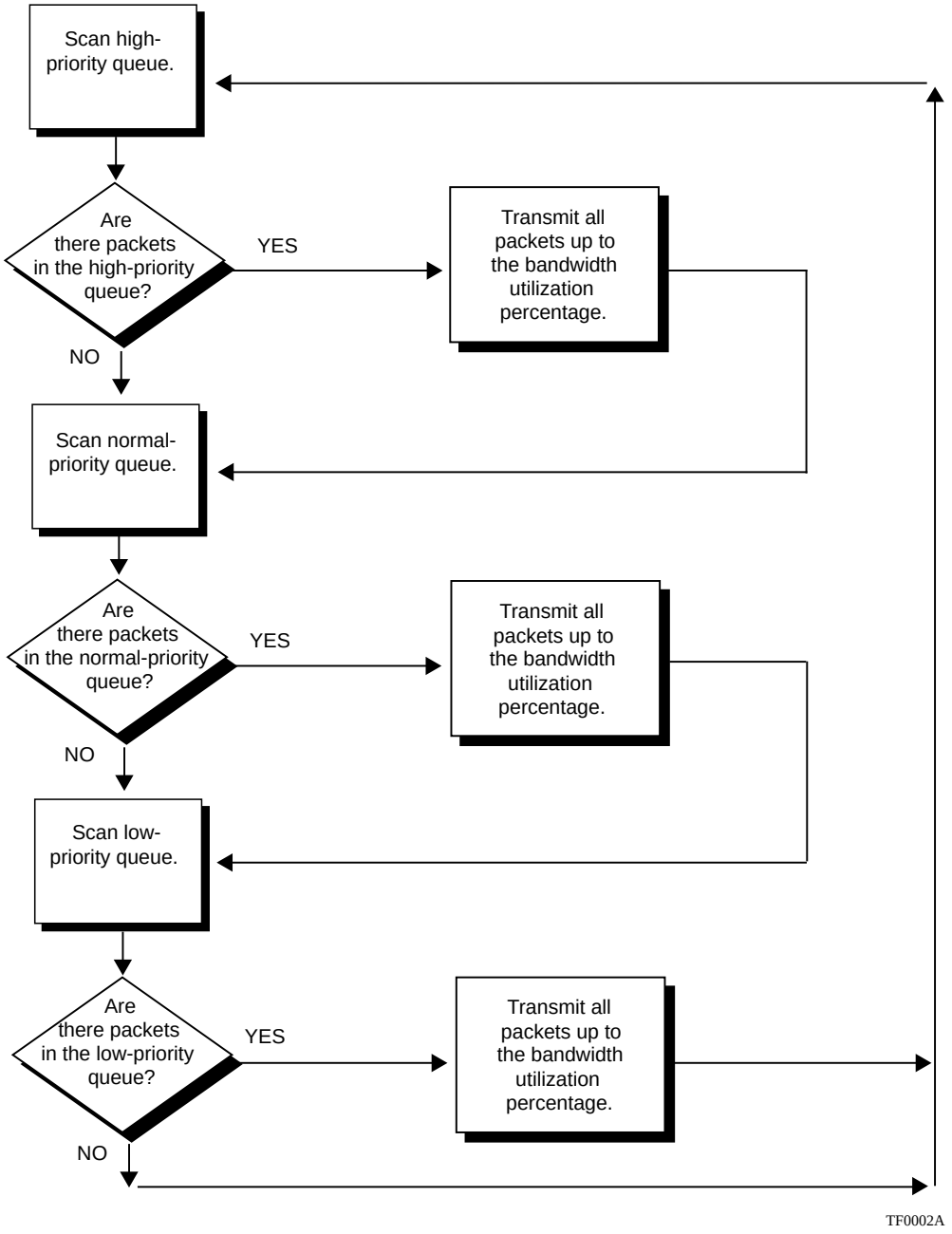
Scan high-priority queue.
Are there packets in the high-priority queue?
YES
Transmit all packets up to the bandwidth utilization percentage.
NO
Scan normal-priority queue.
Are there packets in the normal-priority queue?
YES
Transmit all packets up to the bandwidth utilization percentage.
NO
Scan low-priority queue.
Are there packets in the low-priority queue?
YES
Transmit all packets up to the bandwidth utilization percentage.
NO
TF0002A

Figure 2-2. Bandwidth Allocation Dequeuing Algorithm

Strict Dequeuing Algorithm

Protocol prioritization can also use the strict dequeuing algorithm to send traffic to the transmit queue. This algorithm works as follows:

1. **The transmit queue scans the high-priority queue.**

   If there is no traffic in the high-priority queue, the algorithm proceeds to Step 4.

2. **The router empties all packets from the high-priority queue into the transmit queue, up to the latency value or the maximum transmit queue size, and then transmits them.**

   The transmit queue size is the maximum number of packets in the transmit queue at one time. You cannot configure this number using Site Manager.

3. **If the latency value is reached, the transmit queue starts again, scanning and emptying traffic from the high-priority queue.**

   If neither latency nor the maximum transmit queue size is reached, the algorithm proceeds to Step 4.

4. **The transmit queue scans the normal-priority queue.**

   If there is no traffic in the normal-priority queue, the algorithm proceeds to Step 7.

5. **The router empties all packets from the normal-priority queue, up to the latency value, into the transmit queue and then transmits them.**

6. **If latency is reached, the transmit queue starts again at Step 1, scanning and emptying traffic from the high-priority queue.**

   If latency is not reached, the algorithm proceeds to Step 7.

7. **The transmit queue scans the low-priority queue.**

   If there is no traffic in the low-priority queue, the algorithm starts again at Step 1.

8. **The router empties all packets from the low-priority queue, up to the latency value, into the transmit queue and then transmits them.**

9. **The algorithm starts again at Step 1, whether or not latency is reached.**

Figure 2-3 illustrates the strict dequeuing algorithm.

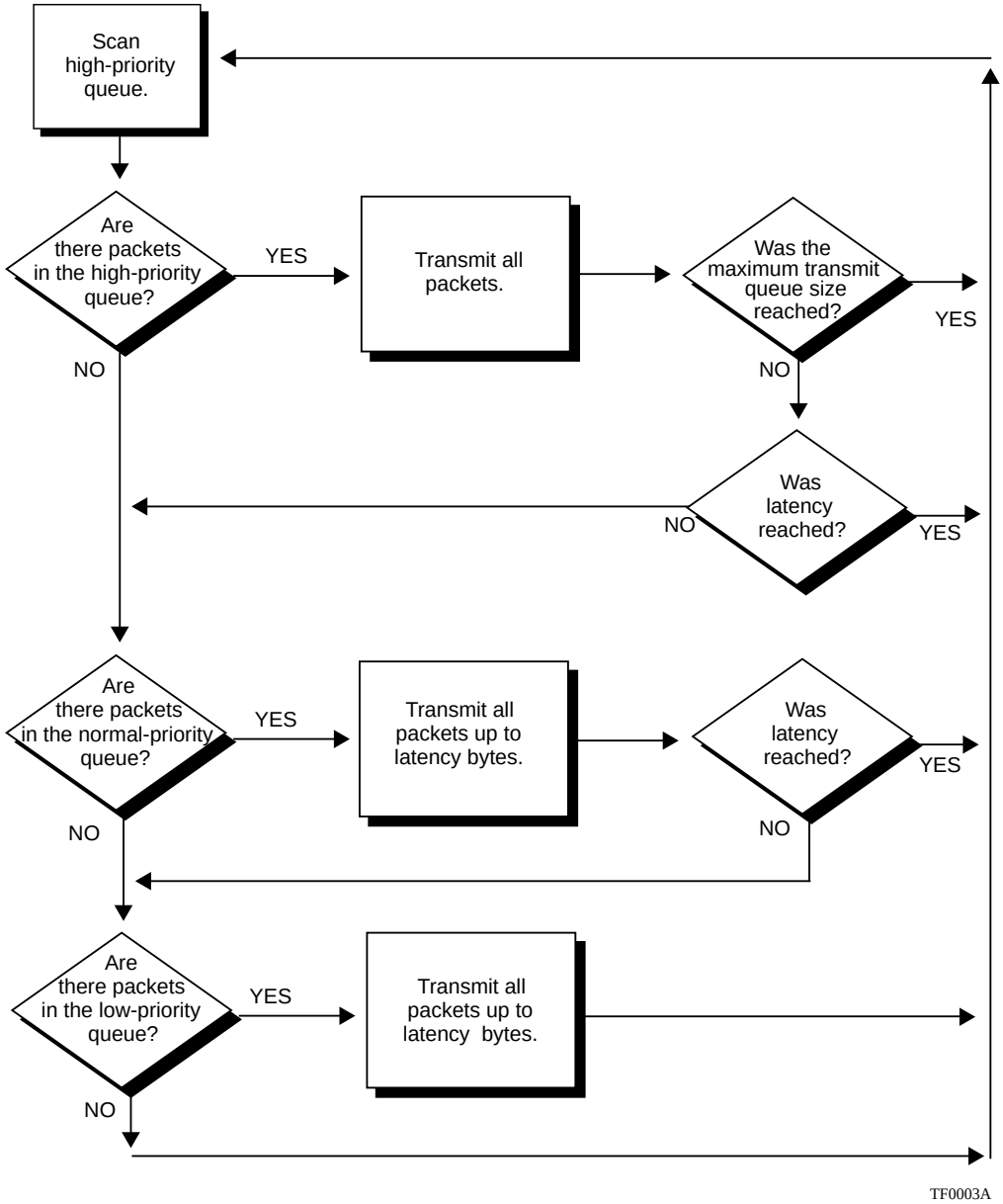

Figure 2-3. Strict Dequeuing Algorithm

Tuning Protocol Prioritization

Protocol prioritization defaults are designed to work well for most configurations. However, you can customize protocol prioritization parameters to maximize its impact in your network.

To set protocol prioritization tuning parameters, use the Edit Protocol Priority Interface window. Refer to “Editing Protocol Prioritization Parameters” later in this chapter for instructions.

Monitoring Statistics

To monitor and manage the impact of protocol prioritization, use the Statistics Manager to view statistics in the MIB object group *wfApplication.wfDatalink.wfProtocolPriorityGroup*. For information on using the Statistics Manager to view MIB objects and create custom screen reports, refer to *Managing Routers and BNX Platforms*.

To determine whether there are enough buffers in each priority queue for the traffic flow on your network, use the Statistics Manager to examine the following protocol prioritization statistics:

- High-Water Packets Mark

  The greatest number of packets that have been in each queue.

- Clipped Packets Count

  The number of packets that have been discarded from each queue. (The router discards packets from full priority queues.)

Note: To determine whether statistics reflect a transient event, you may want to reset the statistics and check again later before changing the configuration of priority queuing. You can reset the High-Water Mark in Site Manager’s Edit Protocol Priority Interface window. You can reset both the Clipped Packets Count and High-Water Packets Mark using the Statistics Manager..

Generally, if a queue’s Clipped Packets Count is high and the High-Water Packets Mark is close to its queue size, that queue does not have enough buffers.

How you tune protocol prioritization depends on whether the bandwidth allocation or strict dequeuing algorithm is active. To tune priority queueing with the bandwidth allocation algorithm active, consider modifying the

- Percent of Bandwidth
- Queue Depth

To improve strict dequeuing results for your protocol prioritization configuration, you can adjust

- Queue Depth
- Latency

Percent of Bandwidth

When using the bandwidth allocation algorithm, you can tune protocol prioritization by changing the default allocation of bandwidth for each of the three priority queues. Queued traffic with large packets often require more than the default bandwidth allocation.

For example, if statistics indicate that one interface requires more than 70 percent of bandwidth to properly transmit high-priority traffic, you can increase the High Queue Size parameter and decrease the Normal or Low Queue Size.

Note: If statistics indicate that the High queue does not have enough buffers, consider reducing the amount of high-priority traffic. You should be selective in assigning high-priority status. Too many traffic types with high-priority status could defeat the purpose of protocol prioritization. With the strict dequeuing algorithm, too much high-priority traffic could result in clipping of normal- and low-priority traffic.

When changing bandwidth allocation, remember that the percent of bandwidth for the High Queue, Normal Queue, and Low Queue must total 100 percent.

Queue Depth

Queue depth (or queue size) is the configurable number of packets that each priority queue can hold. The default value for bandwidth allocation is 20 packets, regardless of packet size.

When you set the queue size, you assign buffers (which hold the packets) to each queue. A queue is full when it exceeds buffer size. The router discards (clips) traffic sent to a full queue.

Note: The buffer size for priority queues is not configurable when using the strict dequeuing algorithm.

Queue Depth Example

Suppose that you use the default queue depth (20 packets) for all three priority queues. You then see from the statistics that the high-priority queue's Clipped Packets Count is 226, and its High-Water Packets Mark is 20. These statistics indicate that the high-priority queue has been full at least once and that the router has discarded 226 packets.

From this information you can conclude that you have not assigned enough buffers to the high-priority queue for the amount of high-priority traffic on this interface.

To prevent further high-priority traffic from being discarded, you can reconfigure the depth of the queues or re-evaluate the amount of traffic assigned to the high-priority queue.

Reconfiguring Queue Depth

Suppose that you now look at the statistics of the normal- and low-priority queues and find that the low-priority queue has a Clipped Packets Count of zero, and a High-Water Packets Mark of 06 (Figure 2-4). Thus, there have never been more than six packets in the low-priority queue, and the router has not discarded any low-priority packets.

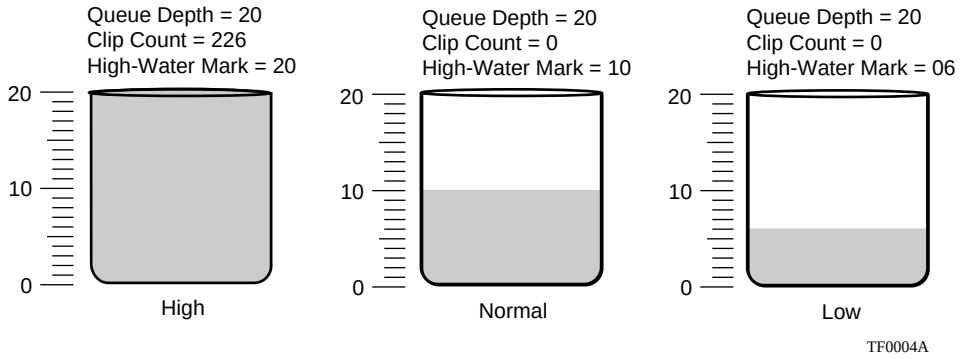

Figure 2-4. Priority Queue Statistics for the Queue Depth Example

In this case, you may choose to reconfigure the low-priority queue depth to 10, and increase the high-priority queue depth to 30 (Figure 2-5).

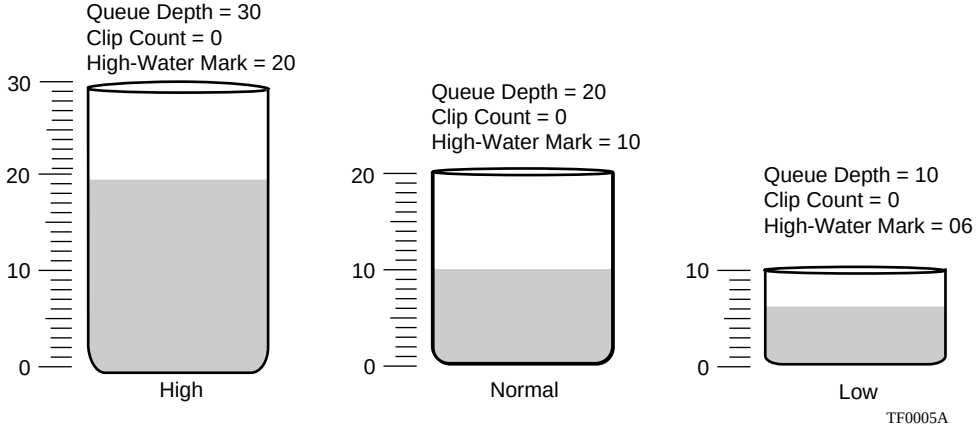

Figure 2-5. Reconfigured Priority Queue Statistics for the Queue Depth Example

To see whether this reallocation solves the problem, reset the Clipped Packets Count and High-Water Packets Mark counters using the Statistics Manager and check them again later.

Latency

Latency, or *line delay*, specifies how many normal- or low-priority bits the router can allocate to the transmit queue at any one time. Latency determines, therefore, the greatest time delay that a high-priority packet can experience.

Latency is based on the line speed of the attached media. The following formula illustrates how line speed, bits queued, and latency value are related.

LATENCY = Bits Queued / Line Speed (bits/s)

The default value for latency is 250 milliseconds (ms). This value usually allows good throughput while preserving rapid terminal response (rapid echoing of keystrokes and timely response to commands) over most media types.

You can change the default latency value. Keep in mind, however, that if you configure a higher latency value (thus allowing more room on the transmit queue), the throughput becomes greater, but you sacrifice terminal response. We recommend accepting the default value of 250 ms.

Enabling Protocol Prioritization

You use the Configuration Manager to configure the high-, normal-, and low-priority queues for circuit-level protocol prioritization. To configure protocol prioritization for a particular interface, you

- Enable protocol prioritization on the circuit -- described in this section.
- Customize the protocol prioritization parameters for the protocol -- described in “Editing Protocol Prioritization Parameters,” later in this chapter.
- Apply an outbound traffic filter to the circuit -- described in Chapter 7.

To enable protocol prioritization:

1. **In the Configuration Manager window, click on the circuit interface connector on which you want to configure Protocol Prioritization.**
2. **Click on Edit Circuit.**

   The Circuit Definition window appears, with the circuit you selected highlighted (Figure 2-6).

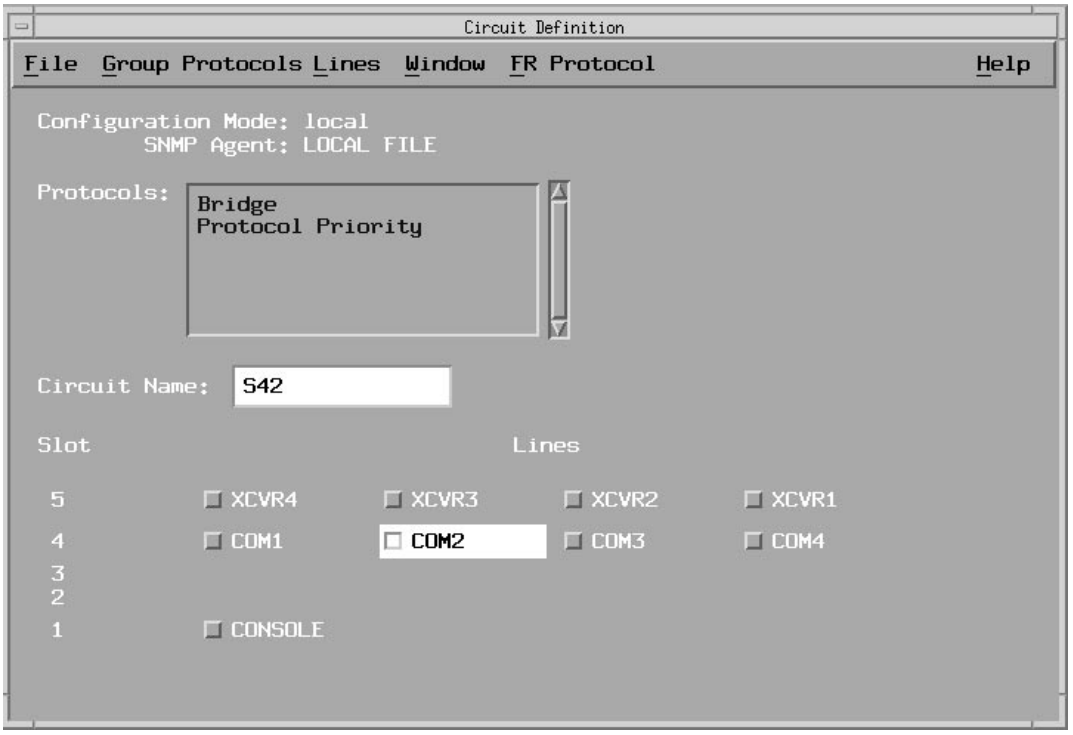

Figure 2-6. Circuit Definition Window

3. **Look for "Protocol Priority" in the Protocols scroll box.**

   If Protocol Priority appears in the Circuit Definition Protocols box (as shown in Figure 2-6), protocol prioritization is already enabled for this interface. (When you select some WAN protocols, Site Manager automatically enables protocol prioritization.)

4. **If Protocol Priority does not appear in the Protocols scroll box, select Protocols > Add/Delete.**

   The Select Protocols window appears (Figure 2-7).

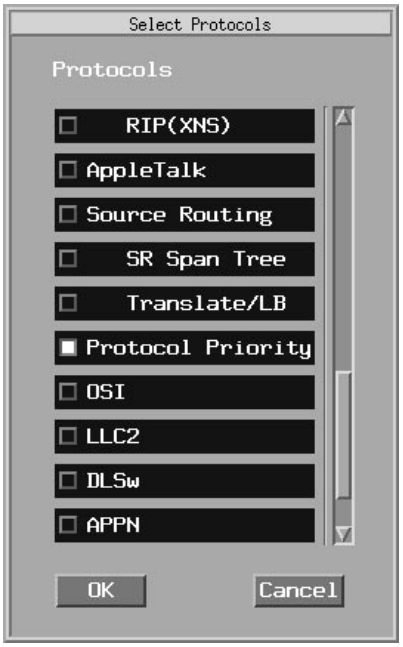

Figure 2-7. Selecting Protocol Priority from the Select Protocols List

5. **Scroll down the list of protocols to select Protocol Priority.**
6. **Click on OK.**

   The Circuit Definition window reappears (refer to Figure 2-6). From the Circuit Definition window, you can

   - Customize parameters, as described in the next section
   - Configure an outbound traffic filter with a priority queue action, as described in Chapter 7

Editing Protocol Prioritization Parameters

Any circuit to which you have added protocol prioritization uses default values that determine how outbound filters work on the interface. You can edit these parameters according to your network traffic needs. To do so, complete the steps in this section.

1. **In the Circuit Definition window, select Protocols > Edit Protocol Priority > Interface (Figure 2-8).**

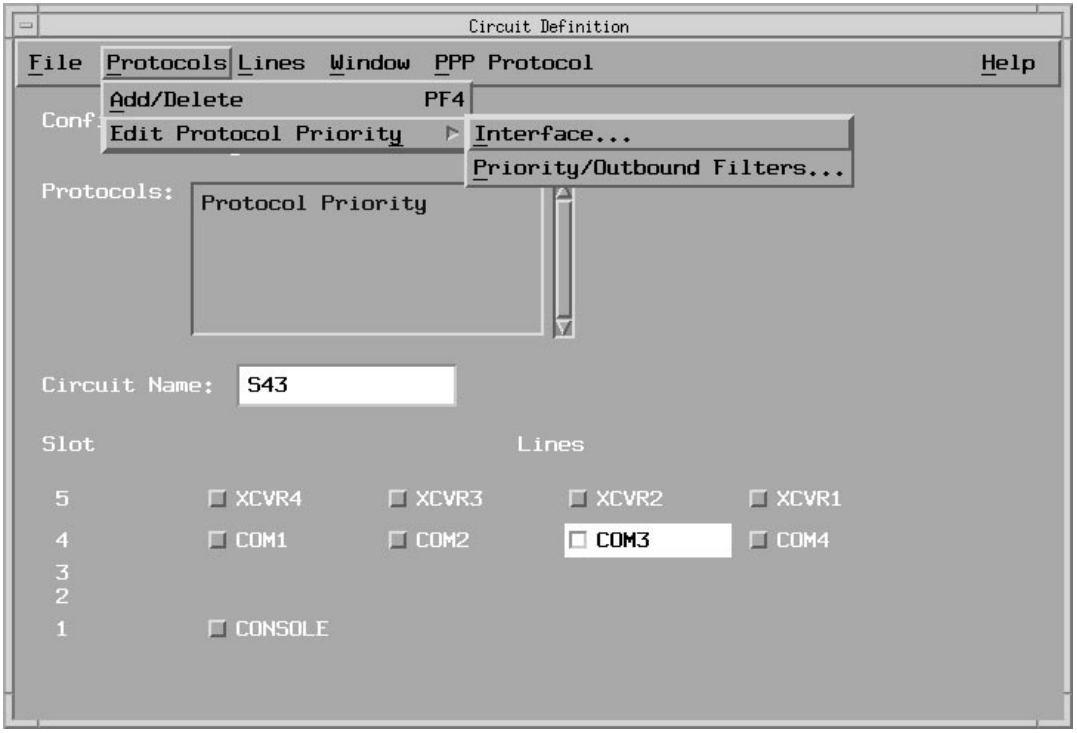

Figure 2-8. Selecting the Edit Protocol Priority Interface Window

The Edit Protocol Priority Interface window appears (Figure 2-9).

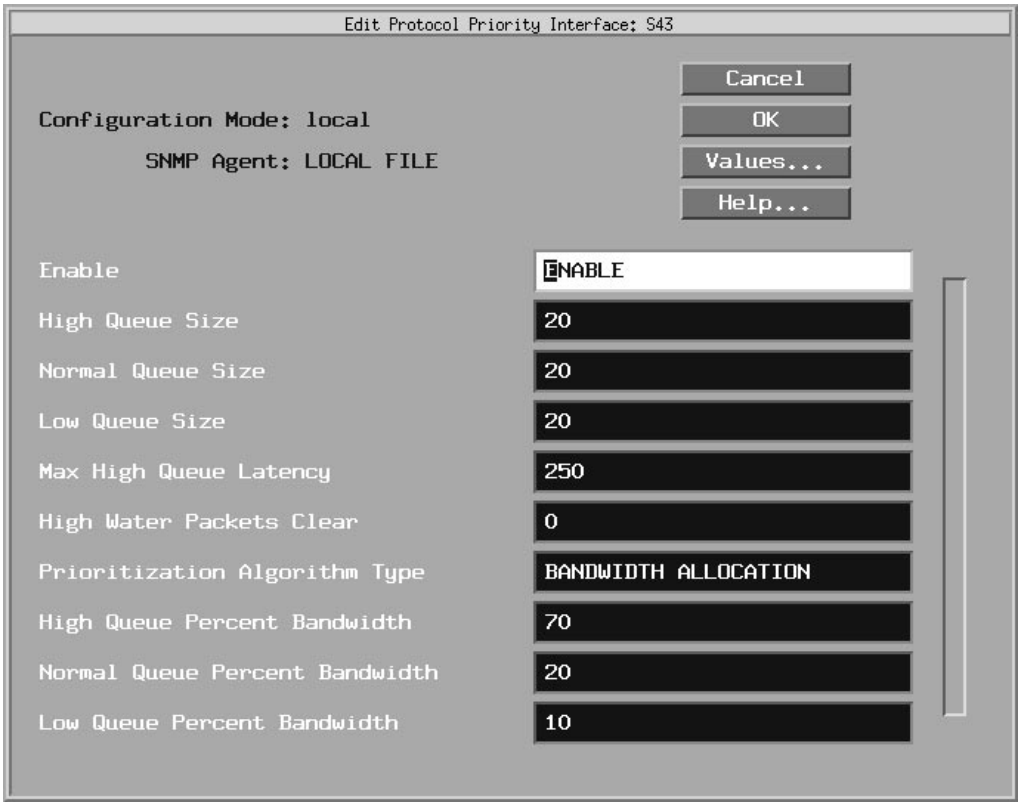

Figure 2-9. Edit Protocol Priority Interface Window (First Screen)

To see additional parameters, use the scroll bar on the right of the window (Figure 2-10).

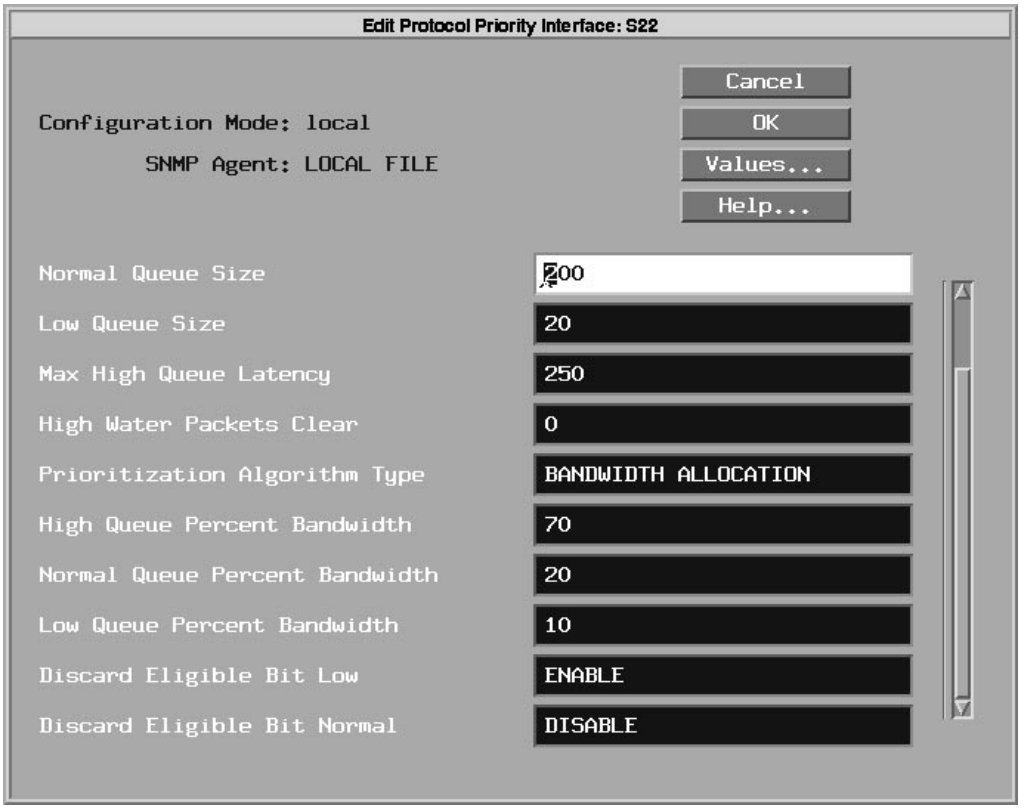

Figure 2-10. Edit Protocol Priority Interface Window (Scrolled Screen)

This window displays parameter values for any interface to which protocol prioritization has been added, whether or not there are any outbound filters currently active on the interface.

2. **Edit the parameters you want to change, using the sections following this procedure as guidelines.**
3. **Click on OK when you are finished editing interface-specific parameters.**

Enabling or Disabling Prioritization

You can toggle protocol prioritization on and off on an interface. If you set the Enable parameter to Disable, all outbound filters are disabled on the interface. Setting this parameter to Disable is useful if you want to temporarily disable all outbound filters rather than delete them.

Set to Enable if you previously disabled protocol prioritization on this interface and now want to re-enable it.

Setting the High Queue Size

By default, there can be up to 20 packets in the high-priority queue at any one time, regardless of packet size. You can specify any integer value as the maximum number of packets in the high-priority queue. For information about using queue depth for tuning protocol prioritization in your network, refer to “Tuning Protocol Prioritization,” earlier in this chapter.

Setting the Normal Queue Size

By default, there can be up to 20 packets (200 for Frame Relay) in the normal-priority queue at any one time, regardless of packet size. You can specify any integer value as the maximum number of packets in the normal-priority queue. For more information about using queue depth for tuning protocol prioritization in your network, refer to “Tuning Protocol Prioritization,” earlier in this chapter.

Note: For Frame Relay interfaces, a value less than 200 might cause a broadcast message to be clipped.

Setting the Low Queue Size

By default, there can be up to 20 packets in the low-priority queue at any one time, regardless of packet size. You can specify any integer value as the maximum number of packets in the low-priority queue. Specifies the maximum number of packets in the low-priority queue at any one time, regardless of packet size. For more information about using queue depth for tuning protocol prioritization in your network, refer to “Tuning Protocol Prioritization,” earlier in this chapter.

Setting the Max High Queue Latency

By default, 250 ms is the greatest delay that a high-priority packet can experience. Consequently, this value determines how many normal-priority or low-priority bits can be in the transmit queue at any one time.

You can accept the default latency of 250 ms, or enter a new latency value between 100 and 5000 ms. We recommend accepting the default value of 250 ms.

For more information about using latency to tune strict dequeuing protocol prioritization in your network, refer to “Latency,” earlier in this chapter.

Clearing the High-Water Mark

When you change the value of this parameter, you reset the High-Water mark for all three priority queues to zero by toggling the High-Water Packets Clear bit. Enter any new integer value for this parameter to clear the existing High-Water marks for the priority queues.

Whenever you change queue depth (by changing the value of the High Queue Size, Normal Queue Size, or Low Queue Size parameter) it’s a good idea to also reset the High-Water mark by changing the value of this parameter.

For more information about using queue depths to tune protocol prioritization in your network, refer to “Tuning Protocol Prioritization,” earlier in this chapter.

Selecting the Prioritization Algorithm Type

You can select one of two dequeuing algorithms for draining priority queues and transmitting traffic.

Select STRICT for strict dequeuing -- the router always transmits traffic in the high-priority queue before traffic in the other queues.

Select BANDWIDTH ALLOC for bandwidth allocation dequeuing -- the router transmits traffic in a queue until the utilization percentage for that queue is reached, and then the router transmits traffic in the next-lower-priority queue. (You configure the percentages for bandwidth allocation by setting the Hiqh Queue, Normal Queue, and Low Queue Percent Bandwidth parameters.)

Setting the High Queue Percent Bandwidth

By default, 70 percent of the bandwidth on an interface is allocated to traffic in the high-priority queue. If you select the bandwidth allocation dequeuing algorithm, you can use this parameter to specify the percentage of bandwidth allocated to high-priority traffic.

When you set this parameter to a value less than 100, each time the percentage of bandwidth used by high-priority traffic reaches this limit, the router transmits traffic in the normal- and low-priority queues, up to the configured percentages for those priority queues.

Note: The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

Setting the Normal Queue Percent Bandwidth

By default, 20 percent of the bandwidth on an interface is allocated to traffic in the normal-priority queue. If you select the bandwidth allocation dequeuing algorithm, you can use this parameter to specify the percentage of bandwidth allocated to normal-priority traffic.

When you set this parameter to a value less than 100, each time the percentage of bandwidth used by normal-priority traffic reaches this limit, the router transmits traffic in the low-priority queues, up to its configured percentage.

Note: The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

Setting the Low Queue Percent Bandwidth

By default, 10 percent of the bandwidth on an interface is allocated to traffic in the low-priority queue. If you select the bandwidth allocation dequeuing algorithm, you can use this parameter to specify the percentage of bandwidth allocated to low-priority traffic. .

Note: The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

Enabling or Disabling the Low-Priority Queue Discard Eligible Bit

By default, Frame Relay packets in the Low priority queue have the Discard Eligible (DE) bit set.

Select DISABLE If you do not want the DE bit to be set for all Frame Relay packets in the Low priority queue

Enabling or Disabling the Normal-Priority Queue Discard Eligible Bit

By default, Frame Relay packets in the Normal priority queue do not have the Discard Eligible (DE) bit set.

Select ENABLE to set the DE bit for all Frame Relay packets in the Normal priority queue.

Chapter 3
Inbound Traffic Filter Criteria and Actions

You create inbound traffic filters from templates that consist of protocol-specific filter criteria, ranges, and actions.

Note: Refer to Chapter 1 for an overview of traffic filters, filter templates, and their criterion, range, and action components.
For instructions on using Site Manager to create inbound filters, see Chapter 6.

To define an inbound traffic filter template, you need to know the specific criteria and actions that Site Manager supports for the applicable protocol. Sections in this chapter lists the predefined inbound traffic filter criteria and actions for all supported bridge and routing protocols, as well as the user-defined reference points for each protocol.

- Transparent Bridge Criteria and Actions
- Source Routing Bridge Criteria and Actions
- DECnet Phase IV Criteria and Actions
- DLSw Criteria and Actions
- IP Criteria and Actions
- IPX Criteria and Actions
- LLC2 Criteria and Actions
- OSI Criteria and Actions
- VINES Criteria and Actions
- XNS Criteria and Actions

Transparent Bridge Criteria and Actions

Transparent bridge traffic filters support multiple encapsulation methods and media types. You filter inbound transparent bridge frames based on header fields within one of the four supported encapsulation methods:

- Ethernet
- IEEE 802.2 logical link control (LLC)
- IEEE 802.2 LLC with Subnetwork Access Protocol (SNAP) header
- Novell Proprietary

Figure 3-1 illustrates the header content of each supported encapsulation method.

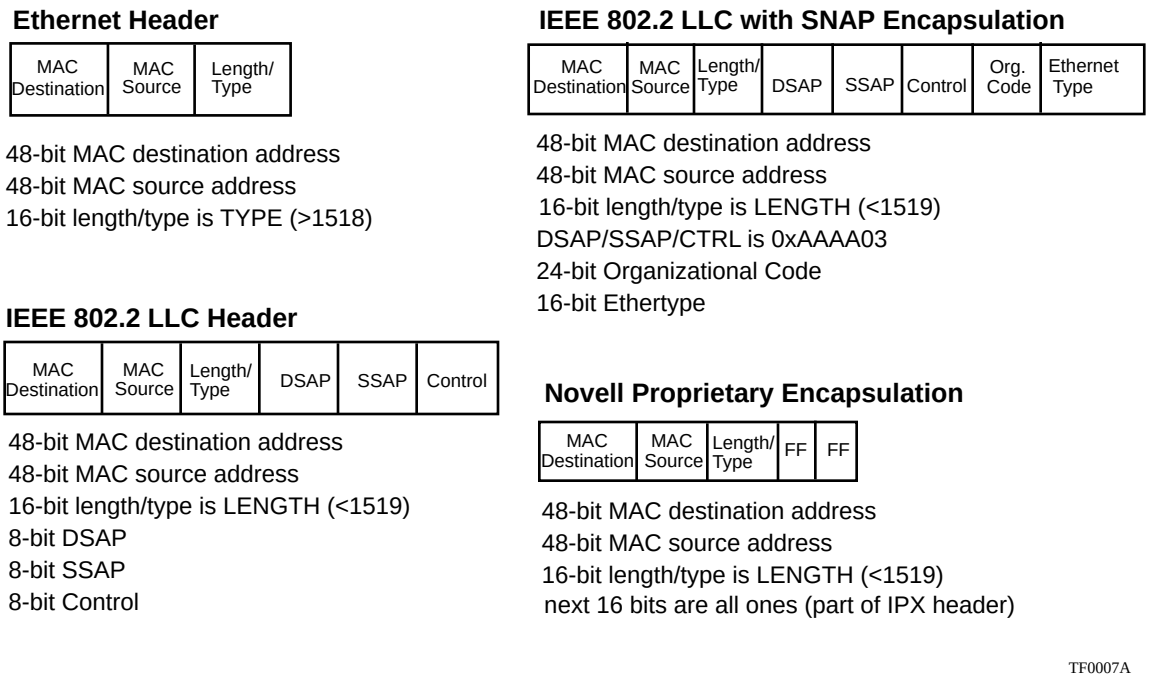

Figure 3-1. Header Reference Fields of Transparent Bridge Encapsulation Methods

Table 3-1 shows which encapsulation methods are supported on specific interface types.

Table 3-1. Bridge Encapsulation Support for Physical Media Types

Router Interface	Bridge Encapsulation Method Supported			
	Ethernet	802.2 LLC	LLC with SNAP	Novell
Ethernet/802.3 (XCVR)	Yes	Yes	Yes	Yes
FDDI (FDDI)	No	Yes	Yes	No
Token Ring (TOKEN)	No	Yes	Yes	No
Synchronous (COM)	Yes	Yes	Yes	Yes

Predefined Transparent Bridge Criteria

Each transparent bridge encapsulation method has specific, predefined criteria for filtering frames. These predefined criteria are based on an offset to a header reference field (see Figure 3-1), and are a specified length. Table 3-2 lists the predefined filtering criteria for each encapsulation method, including the header reference field, offset, and length value for each predefined criterion.

Table 3-2. Predefined Criteria for Transparent Bridge Encapsulations

Encapsulation Method	Criterion Name	Reference Field	Offset (bits)	Length (bits)
All	MAC Source Address	MAC	0	48
	MAC Destination Address	MAC	48	48
Ethernet	Ethernet Type	MAC	96	16
802.2 LLC	Length (Ethernet/802.3 and PPP only)	MAC	96	16
	SSAP	DATA_LINK	0	8
	DSAP	DATA_LINK	8	8
	Control	DATA_LINK	16	8
802.2 LLC with SNAP	Length	MAC	96	16
	Organization Code (Protocol ID)	DATA_LINK	24	24
	Ethernet Type	DATA_LINK	48	16
Novell	Novell	MAC	112	16

User-Defined Transparent Bridge Criteria

You can create bridge traffic filters with user-defined criteria by specifying an offset and length to these supported reference fields:

Reference Field	Description
MAC	Points to the first byte of the Destination MAC address
DATA_LINK	Points to the first byte of the DATA_LINK reference field

Transparent Bridge Actions

In addition to the Accept, Drop, and Log actions that are common to all the protocols, there are two Bridge-specific actions:

- Flood

  Specifies that any frame that matches the filter will be forwarded onto all Bridge circuits except for the circuit from which it was received.

- Forward to Circuit List

  Specifies that any frame that matches the filter will be forwarded to certain circuits that you specify.

Note: The circuit names that you enter in the Forward to Circuit List window are case-sensitive. For example, if the circuit name is E21, you must enter it as **E21**, not **e21**, or the filter will not work.

You can combine the Log action with any of the other actions. However, you should use Log only to record abnormal events; otherwise, the event log will fill up with filtering messages and thus become useless.

Source Routing Bridge Criteria and Actions

You filter inbound Source Routing traffic based on specified bit patterns contained within the native source routing bridge (SRB) frame header. IP-encapsulated SRB traffic filters are not supported.

Source Routing filters affect both explorer and routed frames. However, filters that include Next Ring as a criterion affect only routed frames, because the Next Ring reference field does not appear in explorer frames. Refer to *Configuring Bridging Services* for information about explorer and routed frames.

Note: The router applies source route bridge filters *after* the router processes a packet. The router receives the packet on the incoming interface and updates the routing information field (RIF). The filters that you configure then act on the updated RIF.

Predefined Source Routing Criteria

Table 3-2 lists the predefined filtering fields for Source Routing filters and the SRB header reference field, offset, and length value for each criterion.

Table 3-3. Predefined Criteria for Source Routing Bridge

Criterion Name	Reference Field	Offset (bits)	Length (bits)
Next Ring	NEXT_RING	0	12
Destination MAC Address	HEADER_START	0	48
Source MAC Address	HEADER_START	48	48
DSAP	DATA_LINK	0	8
SSAP	DATA_LINK	8	8
Destination NetBIOS Name	DATA_LINK	120	120
Source NetBIOS Name	DATA_LINK	248	120

Specifying a SRB Criterion Range

If you create a filter that includes a Source or Destination NetBIOS Name (Source Routing protocol), you enter the NetBIOS name as the ASCII equivalent of the first 15 characters of the name. If the name has fewer than 15 characters, use ASCII spaces (0x20) to ensure that the name has 15 characters.

Refer to Chapter 5 for information about entering SAP and MAC address criteria.

User-Defined Source Routing Criteria

In addition to the predefined filter criteria, you can create SRB traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the source routing header:

Reference Field	Description
NEXT_RING	Points to the first byte of the Next Ring field
HEADER_START	Points to the first byte of the Destination MAC address
DATA_LINK	Points to the first byte of the DATA_LINK reference field

Source Routing Actions

In addition to the Accept, Drop, and Log actions common to all protocols, Source Routing supports two additional actions:

- Direct IP Explorers

  Specifies that any explorer frame that matches the filter will be sent to some number of IP addresses. You are required to specify these IP addresses.

  For this action to work, IP encapsulation must be configured on the filter's interface. If IP encapsulation is not configured and a frame matches the filter, the frame will be flooded as if no filter existed.

- Forward to Circuits

  Specifies that any frame that matches the filter will be forwarded to certain circuits that you specify.

Note: The circuit names you enter in the Forward to Circuit list are case-sensitive. For example, if the circuit name is E21, but you enter it as **e21**, the filter will not be saved.

DECnet Phase IV Criteria and Actions

You can filter inbound DECnet Phase IV traffic based on specified bit patterns contained within the DECnet header.

Predefined DECnet Criteria

Table 3-2 lists the predefined filtering fields for DECnet IV inbound traffic filters and the reference field, offset, and length value for each criterion.

Table 3-4. Predefined Criteria for DECnet Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination Area	DEC4_BASE	0	6
Destination Node	DEC4_BASE	6	10
Source Area	DEC4_BASE	16	6
Source Node	DEC4_BASE	22	10

User-Defined DECnet Criteria

In addition to the predefined DECnet filter criteria, you can create traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the DECnet Phase IV header:

Reference Field	Description
DEC4_BASE	Points to the first byte in the header

DECnet Actions

The DECnet Phase IV filtering actions are Accept, Drop, and Log.

DLSw Criteria and Actions

You can filter inbound DLSw traffic based on specified bit patterns contained within the DLSw header, as defined in RFC 1434.

Predefined DLSw Criteria

Table 3-2 lists the predefined filtering fields for DLSw inbound traffic filters and the reference field, offset, and length value for each criterion.

Table 3-5. Predefined Criteria for DLSw Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination MAC Address	DLS_BASE	192	48
Source MAC Address	DLS_BASE	240	48
DSAP	DLS_BASE	296	8
SSAP	DLS_BASE	288	8

User-Defined DLSw Criteria

In addition to the predefined DLSw filter criteria, you can create inbound traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the DLSw header:

Reference Field	Description
DLS_CTRL_START	Points to the start of the DLSw header
DLS_DATA_START	Point to start of the DLSw data

DLSw Actions

The DLSw filtering actions are

- Drop, Log -- common to all inbound traffic filters
- Forward to Peer -- specifies that any frame that matches the filter will be sent to the circuits that you specify

IP Criteria and Actions

You filter inbound IP traffic based on specified bit patterns contained within the IP header or the header of the upper-level protocol (TCP or UDP, for example) conveyed within the IP datagram.

Predefined IP Criteria

Table 3-2 lists the predefined filtering fields for IP filters and the reference field, offset, and length value for each criterion.

Table 3-6. Predefined Criteria for IP Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Type of Service	HEADER_START	8	8
Protocol	HEADER_START	72	8
IP Source Address	HEADER_START	96	32
IP Destination Address	HEADER_START	128	32
UDP/TCP Source Port	HEADER_END	0	16
UDP/TCP Destination Port	HEADER_END	16	16

User-Defined IP Criteria

In addition to the predefined filter criteria, you can create IP traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the IP header:

Reference Field	Description
HEADER_START	Points to the first byte of the Type of Service
HEADER_END	Points to the last byte of the IP Destination Address

Note: When specifying IP user-defined criteria, use 8-bit lengths whenever possible. User-defined IP traffic filters one bit long work only when aligned on a byte (word) boundary. Lengths from 2 to 7 bits do not work.

IP Actions

In addition to the Accept, Drop, and Log actions common to all the protocols, IP supports the following actions:

- Forward to Next Hop

  Specifies that any frame that matches the filter will be forwarded to the next-hop router. You must specify the IP address of the next-hop router. If the next-hop router is not reachable, any packets matching the filter will be forwarded normally unless you also specify Drop If Next Hop Is Unreachable.

  If you specify 255.255.255.255 as the Next Hop, then any frame that matches this filter will be forwarded normally.

- Drop If Next Hop Is Unreachable

  This action is valid only when Forward to Next Hop is in use. Specifies that if the next-hop address specified is unreachable, the frame is dropped.

- Forward to IP Address

  Specifies that any frame that matches the filter will be forwarded to a single address in a list of specified IP addresses. The destination address of the original packet changes to the specified IP address.

- Forward to Next Hop Interfaces

  Specifies that any frame that matches the filter will be duplicated and forwarded to a group of next-hop interfaces based on a list of IP addresses you specify. If none of the next-hop interfaces is up, any packets matching the filter will be forwarded to the default destination for the packet destination address (unless you also specify Drop If Next Hop Is Unreachable).

- Forward to First Up Next Hop Interface

  Ensures traffic forwarding by specifying that any frame that matches the filter will be forwarded to a specified next-hop router or network connected to the router. If the specified hop is not reachable, the filter tries all addresses on the next-hop interfaces list using ARP (Address Resolution Protocol) messages. If none of the next-hop interfaces is reachable, any packets matching the filter will be forwarded to the default destination for the packet destination address (unless you also specify Drop If Next Hop Is Unreachable).

- Detailed Logging

  For every packet that matches the filter criteria and ranges, the filter adds an entry containing IP header information to the system Events log.

IPX Criteria and Actions

You filter inbound IPX traffic based on specified bit patterns contained within the IPX header.

Predefined IPX Criteria

Table 3-2 lists the predefined filtering fields for IPX filters and the reference field, offset, and length value for each criterion.

Table 3-7. Predefined Criteria for IPX Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination Network	IPX_BASE	48	32
Destination Address	IPX_BASE	80	48
Destination Socket	IPX_BASE	128	16
Source Network	IPX_BASE	144	32
Source Address	IPX_BASE	176	48
Source Socket	IPX_BASE	224	16

User-Defined IPX Criteria

In addition to the predefined filter criteria, you can create traffic filters with criteria you define by specifying an offset and length to the start of the IPX header (IPX_BASE) as a reference field for a user-defined criterion.

Reference Field	Description
IPX_BASE	Points to the first byte in the IPX header

IPX Actions

The IPX filtering actions are Accept, Drop, and Log.

LLC2 Criteria and Actions

You can filter inbound LLC2 traffic based on specified bit patterns contained within the LLC2 header. Adding an IBM protocol to a circuit automatically adds Logical Link Control 2 (LLC2). LLC2 traffic filters apply to LLC2 routed over Frame Relay (also known as native SNA over Frame Relay) and to any protocol running over LLC2, including Advanced Peer-to-Peer Networking (APPN) and LAN Network Manager (LNM).

Predefined LLC2 Criteria

Table 3-2 lists the predefined filtering fields for DLSw inbound traffic filters and the reference field, offset, and length value for each criterion.

Table 3-8. Predefined Criteria for LLC2 Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination MAC Address	LLC2_DEST_MAC	0	48
Source MAC Address	LLC2_SOURCE_MAC	48	48
DSAP	LLC2_DSAP	0	8
SSAP	LLC2_SSAP	8	8

User-Defined LLC2 Criteria

You can create traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the LLC2 header:

Reference Field	Description
LLC2_DEST_MAC	Points to the first byte of the Destination MAC address
LLC2_DSAP	Points to the first byte of the Destination SAP

LLC2 Actions

The LLC2 filtering actions are Accept, Drop, and Log.

OSI Criteria and Actions

You can configure OSI inbound traffic filters based on specified bit patterns contained within the CLNP header.

Predefined OSI Criteria

Table 3-2 lists the predefined filtering fields for OSI inbound traffic filters and the reference field, offset, and length value for each criterion.

Table 3-9. Predefined Criteria for OSI Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination Area	OSI_DEST	0	16
Destination System ID	OSI_DEST	16	48
Source Area	OSI_SRC	0	16
Source System ID	OSI_SRC	16	48

User-Defined OSI Criteria

In addition to the predefined OSI filter criteria, you can create traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the OSI header:

Reference Field	Description
OSI_BASE	Points to the first byte of the CLNP header
OSI_DEST	Points to the last two bytes of the Destination Address field
OSI_SRC	Points to the last two bytes of the Source Address field

OSI Actions

The OSI filtering actions are Accept, Drop, and Log.

VINES Criteria and Actions

You can configure VINES inbound traffic filters based on specified bit patterns contained within the VINES IP header.

Predefined VINES Criteria

Table 3-2 lists the predefined filtering fields for VINES inbound traffic filters and the reference field, offset, and length value for each criterion.

Table 3-10. Predefined Criteria for VINES Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Protocol Type	VINES_BASE	40	8
Destination Address	VINES_BASE	48	48
Source Address	VINES_BASE	96	48

User-Defined VINES Criteria

In addition to the predefined VINES filter criteria, you can create traffic filters with user-defined criteria by specifying an offset and length to these reference fields in the VINES header:

Reference Field	Description
VINES_BASE	Points to the first byte in the header

VINES Actions

The VINES filtering actions are Accept, Drop, and Log.

XNS Criteria and Actions

You can configure XNS inbound traffic filters based on specified bit patterns contained within the XNS header.

Predefined XNS Criteria

Table 3-2 lists the predefined filtering fields for XNS filters and the reference field, offset, and length value for each criterion.

Table 3-11. Predefined Criteria for XNS Inbound Traffic Filters

Criterion Name	Reference Field	Offset	Length
Destination Network	XNS_BASE	48	32
Destination Address	XNS_BASE	80	48
Destination Socket	XNS_BASE	128	16
Source Network	XNS_BASE	144	32
Source Address	XNS_BASE	176	48
Source Socket	XNS_BASE	224	16

User-Defined XNS Criteria

In addition to the predefined filter criteria, you can create traffic filters with criteria you define by specifying an offset and length to the start of the XNS header (XNS_BASE) as a reference field for a user-defined criterion.

Reference Field	Description
XNS_BASE	Points to the first byte in the XNS header

XNS Actions

The XNS filtering actions are Accept, Drop, and Log.

Chapter 4
Outbound Traffic Filter Criteria and Actions

This chapter lists the filter criteria and actions that Site Manager supports for outbound traffic filters.

Note: For information about DLSw outbound filters, refer to the *Configuring DLSw Services* guide.

As described in Chapter 1, you create protocol-specific filter templates that include either predefined criteria or criteria you define from supported reference points in the protocol header (*user-defined criteria*).

Sections of this chapter define

- Predefined Criteria
- Reference Points for User-Defined Criteria
- Actions for Outbound Traffic Filters

Note: In some configurations, implementing outbound traffic filters for LAN protocols may cause a decline in throughput performance. For LAN circuits where the forwarding rate of the router is critical, we suggest that you monitor the throughput performance after configuring outbound LAN filters. If you notice an unacceptable performance degradation, use inbound traffic filters to accomplish the filtering goal.

For instructions on using Site Manager to create outbound filters, see Chapter 7.

Predefined Criteria

Outbound traffic filter criteria are based on a packet's Data Link or IP header.

- For most WAN and LAN routing protocols, you can use predefined outbound filter criteria based on either the Data Link header *or* the IP protocol header.
- For bridge traffic, all predefined criteria are part of the Data Link header only.
- For NetBIOS, SNA, and other DLSw-encapsulated traffic, predefined criteria for outbound filters are based on the DLSw protocol header. For information about DLSw outbound filters, refer to the *Configuring DLSw Services* guide.

This section explains

- Predefined Data Link Criteria
- Predefined IP Criteria
- Specifying Criteria Common to IP and Data Link Headers

Predefined Data Link Criteria

You can configure outbound filters based on the predefined Data Link header criteria listed in Table 4-1.

Table 4-1. Predefined Data Link Outbound Filter Criteria

Packet Type or Component	Predefined Criteria
Data Link Type	MAC Source Address MAC Destination Address Ethernet Type Novell 802.2 Length 802.2 DSAP 802.2 SSAP 802.2 Control 802.2 SNAP Length 802.2 SNAP Protocol ID 802.2 SNAP Ethernet Type (Ethertype)
Source Routing	DSAP SSAP

(continued)

Table 4-1. Predefined Data Link Outbound Filter Criteria *(continued)*

Packet Type or Component	Predefined Criteria
PPP	Protocol ID
Frame Relay	2-byte DLCI 3-byte DLCI 4-byte DLCI NLPID Ethernet Type (Ethertype)

Figure 4-1 shows the Configuration Manager menu path for specifying these criteria. See Chapter 7 for detailed instructions on creating outbound filters.

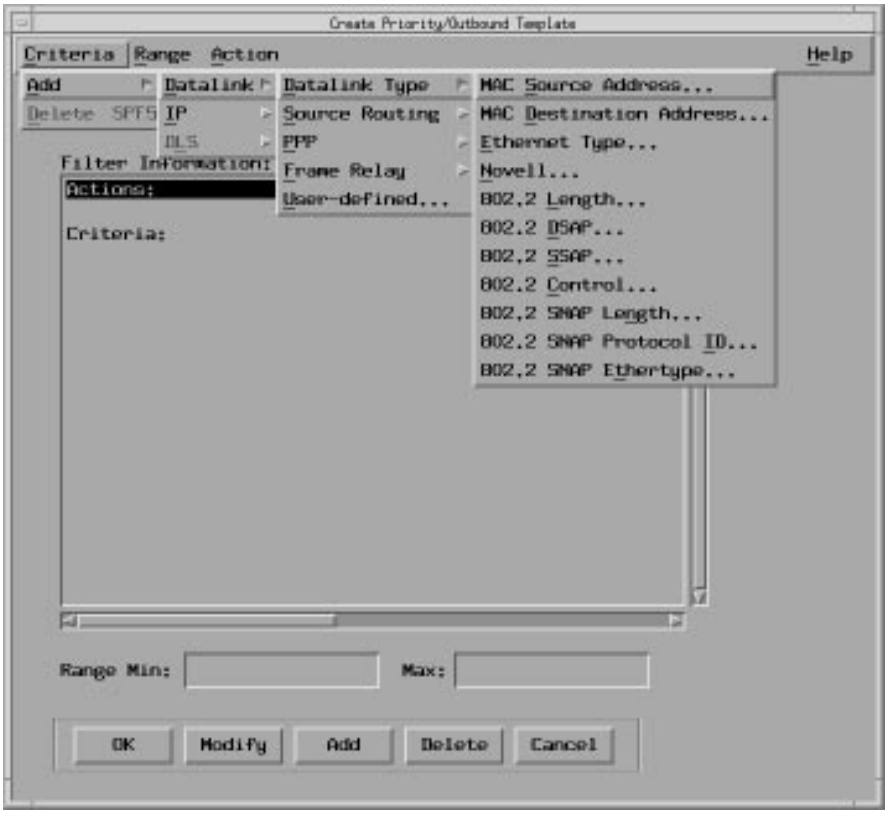

Figure 4-1. Predefined Data Link Outbound Filter Criteria

Predefined IP Criteria

You configure outbound filters for routing protocols based on the predefined criteria listed in Table 4-2.

Table 4-2. Predefined IP Outbound Filter Criteria

Packet Type or Component	Predefined Criteria
IP Header	Type of Service IP Source Address IP Destination Address Both Source Address *and* Destination Address UDP Source Por UDP Destination Port TCP Source Port TCP Destination Port TCP *or* UDP Source Port TCP *or* UDP Destination Port Established TCP Port Protocol
Source Routing	MAC Destination Address MAC Source Address SSAP DSAP
PPP	Protocol ID
Frame Relay	2-byte DLCI 3-byte DLCI 4-byte DLCI NLPID

Figure 4-2 shows the Configuration Manager menu path for specifying these criteria. See Chapter 7 for detailed instructions on using Configuration Manager to create outbound filters.

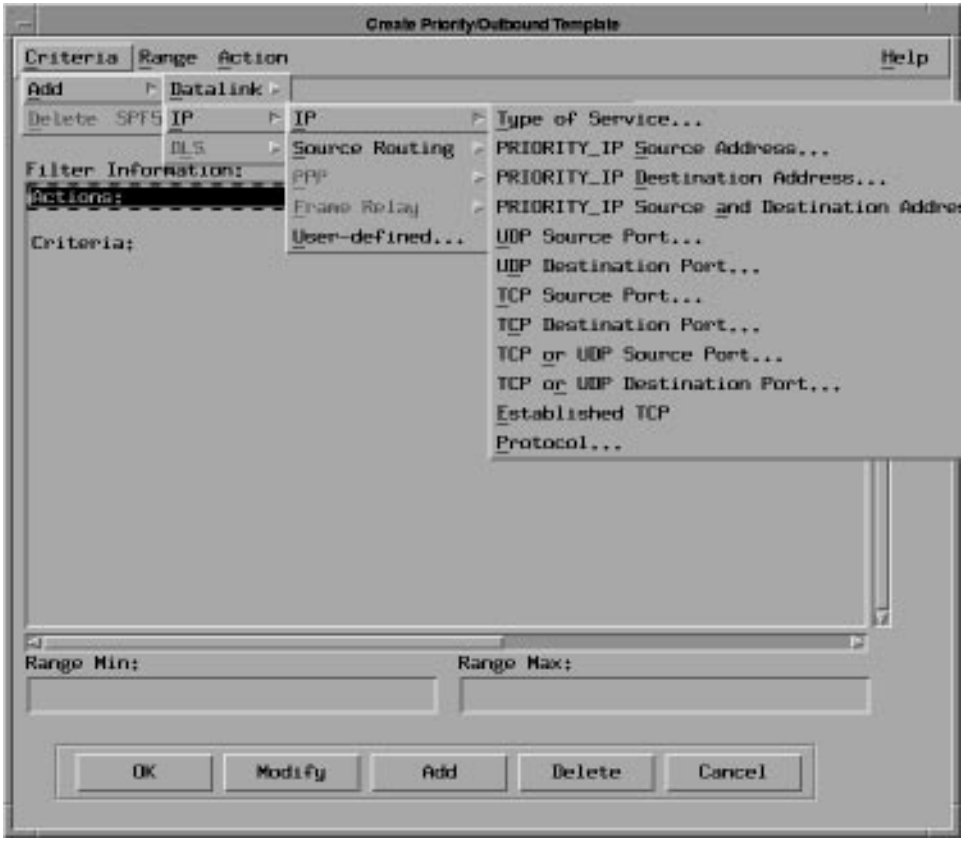

Figure 4-2. Predefined IP Outbound Filter Criteria

Specifying Criteria Common to IP and Data Link Headers

To configure outbound filters for criteria that are common to both IP and Data Link headers (DSAP, SSAP, Protocol ID, DLCI, NLPID), create two filters: one for IP and the other for the Data Link type. For example, if you want a filter rule with a priority of High for all Frame Relay traffic with DLCI 400, create filters for both IP and Data Link using the DLCI criterion and a range of 400.

To configure a filter to apply to either the IP or Data Link header only, create only one filter.

To configure filters for IP-routed packets only, always select IP instead of Data Link. If you create a filter under Data Link to identify an IP-routed packet (for example, using the Ethertype field and a value of 0x0800), the rule is never triggered because the router code recognizes the IP packet and uses IP filter rules.

Reference Points for User-Defined Criteria

To create a filter with a user-defined criterion, you specify the offset and length to a supported reference point in the protocol's header. This section lists reference points for specifying user-defined outbound traffic filter criteria:

- Data Link Reference Points
- IP Reference Points

Data Link Reference Points

Table 4-3 defines the Data Link reference points.

Table 4-3. Data Link Reference Points

Reference Point	Definition
MAC	Points to the high-order byte of the destination address
DATA_LINK	Points to the first byte after the length/type criteria
DL_HEADER_START	Points to the beginning of the header (beginning of the packet) for PPP and Frame Relay
DL_HEADER_END	Points to the first byte after DLCI in Frame Relay and the first byte after the protocol ID in PPP
DL_FR_MPE	Points to NLPID (Frame Relay only)
DL_SR_START	Points to the beginning of the source routing packet, which is the high-order byte of the destination address
DL_SR_DATA_LINK	Points to the first byte after the RIF field

Figures 4-3 and 4-4 show examples of where those reference points are located in a packet.

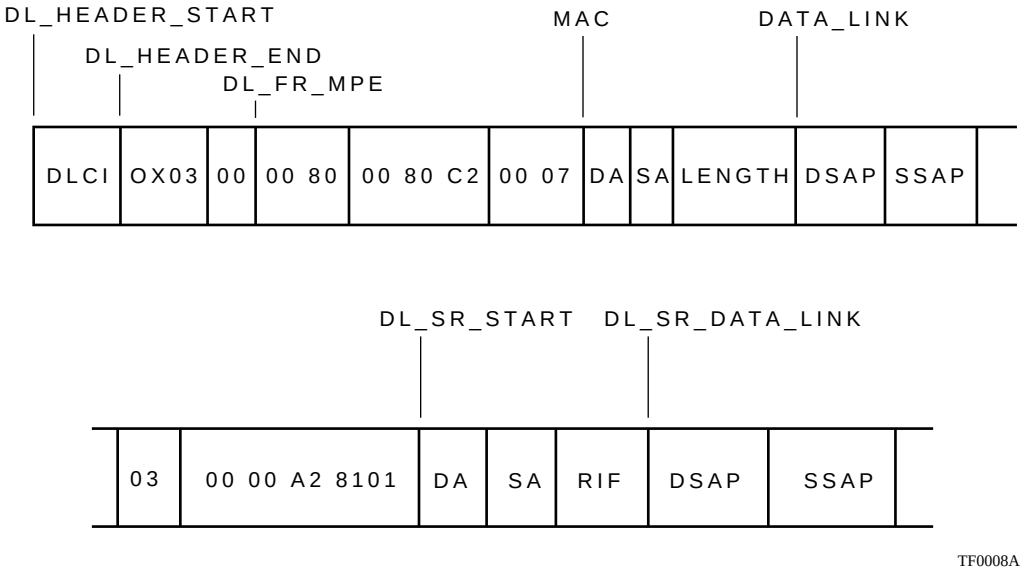

Figure 4-3. Data Link Reference Points in a Source Routing Packet Bridged over Bay Networks Proprietary Frame Relay

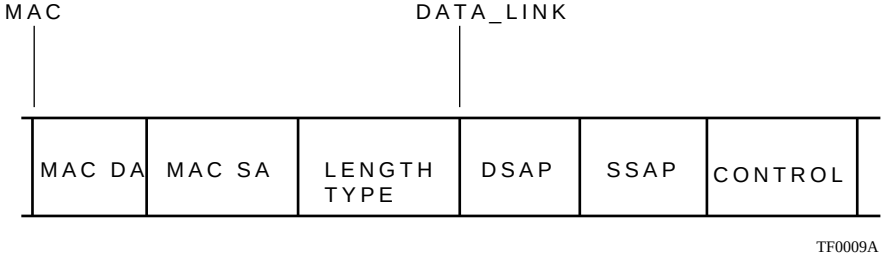

Figure 4-4. Data Link Reference Points in an IEEE 802.2 LLC Header

IP Reference Points

Table 4-4 defines the IP reference points, and Figure 4-5 shows an example of where those reference points are located in a packet.

Table 4-4. IP Reference Points

Reference Point	Definition
HEADER_START	Points to the first byte in the IP header
HEADER_END	Points to the first byte after the IP header
IP_WAN_HEADER_START	Points to the beginning of the header (beginning of the packet) for PPP and Frame Relay
IP_WAN_HEADER_END	Points to the first byte after DLCI in Frame Relay and the first byte after the Protocol ID in PPP
IP_SR_START	Points to the beginning of the source routing packet, which is the high-order byte of the destination address
IP_SR_DATA_LINK	Points to the first byte after the RIF field

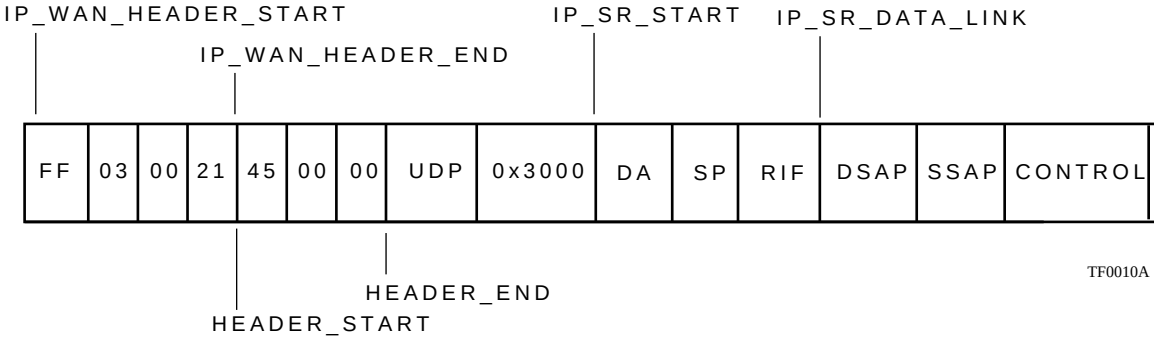

Figure 4-5. IP Reference Points in a PPP Packet with IP Encapsulated Source Routing

Actions for Outbound Traffic Filters

For outbound traffic filters, you can specify different types of actions:

- Filtering Actions
- Protocol Prioritization Actions
- Dial-On-Demand Actions

Filtering Actions

You can apply the following actions to any outbound traffic filter:

- Accept -- The router processes any packet that matches the filter criteria and ranges.
- Drop -- The router does not route any packet that matches the filter criteria and ranges.
- Log -- For every packet that matches the filter criteria and ranges, the router sends an entry to the system Events log. You can specify the Log action in combination with other actions.
- Detailed Log -- For every packet that matches the filter criteria and ranges, the filter adds a more detailed entry to the system Events log, containing IP header information.

Note: Specify the Log actions only to record abnormal events; otherwise, the Events log will fill up with filtering messages, leaving no room for critical log messages.

Protocol Prioritization Actions

Outbound traffic filters for WAN protocols also include the following actions for directing matching traffic into circuit-based protocol priority queues:

- High -- Packets that match the filter criteria and ranges are processed in the high queue.
- Low -- Packets that match the filter criteria and ranges are processed in the low queue.
- Length -- For packets that match the filter criteria, the packet length determines the priority queue into which it is placed.

Dial-On-Demand Actions

On lines configured for Dial-on-Demand (DoD), all packets transmitted will trigger the router to establish a connection. With Dial Optimized Routing implemented, a connection is not always necessary for the usual routing packets, such as IP RIP or IPX RIP/SAP.

You can use dial-on-demand actions to specify packet types that should not bring up a dial connection or reset the inactivity timer.

- No Call -- Packets that match the filter criteria and ranges are dropped and do not initiate a dial connection.
- No Reset -- Packets that match the filter criteria and ranges are processed but do not reset the inactivity timer.

See *Configuring Dial Services* for information about dial services such as DoD and Dial Optimized Routing.

Chapter 5
Specifying Common Criterion Ranges

For every inbound or outbound traffic filter criterion, you must specify a valid *range* -- a series of target values appropriate to the criterion. For many criteria, you specify an address range.

This chapter lists valid range values for common traffic filter criteria and explains how to specify common address ranges in the following sections:

- Specifying MAC Address Ranges
- Specifying VINES Address Ranges
- Specifying Source and Destination SAP Code Ranges
- Specifying Frame Relay NLPID Range Values
- Specifying PPP Protocol ID Range Values
- Specifying TCP and UDP Port Range Values
- Specifying Ethernet Type Range Values
- Specifying IP Codes

Note: Refer to Chapter 1 for an overview of traffic filters, filter templates, and their criterion, range, and action components.

Specifying MAC Address Ranges

When you create a filter that includes a Source or Destination MAC Address criterion, you specify the MAC address range in either most-significant-bit (MSB) or canonical format. Table 5-1 lists the address formats to use.

Table 5-1. Format for Specifying Source-Routing MAC Addresses

Address Type	Address Format
PPP	MSB
Bay Networks Standard Frame Relay	Canonical
Bay Networks Proprietary PPP	Canonical
Token Ring	MSB
Ethernet	Canonical

When defining outbound traffic filters you can specify a MAC address in either MSB or canonical format, but the default is canonical.

Source Routing Bridge Source MAC Addresses

When specifying Source MAC addresses for SRB traffic filters, set the most significant bit (MSB) to one.

For example (Token Ring packets):

1. The Source MAC address to be filtered is 0x40000037450440.
2. Add the First Bit Set MAC Address 0x800000000000.
3. Enter the filter criteria range as 0xC00037450440.

Bit 0 (the 0x80 bit) of Byte 0 (the leftmost byte) is the Routing Information Indicator bit, which indicates the presence of the Routing Information Field (RIF). This bit is set to 1 if the RIF is present and to 0 if there is no RIF. Keep this in mind if you use a sniffer to analyze packets for their Source MAC address. For example, a sniffer would decode LAA with the first byte of 40 as 0x400031740001. If the RIF bit is set, the hexadecimal value of the packet is 0xC00031740001.

Source Routing Bridge Functional MAC Addresses

Functional MAC addresses are Destination MAC addresses that always conform to the following rules:

- Byte 0 = 0xC0
- Byte 1 = 0x00
- The first half of byte 2 = 0x0 to 0x7

Table 5-2 lists some common functional MAC addresses.

Table 5-2. Functional MAC Addresses

Function Name	MAC Address (MSB)	Identifying Bit	Ethernet Address
Active Monitor	0xC000 0000 0001	Byte 5, bit 7	0x030000000080
Ring Parameter Server	0xC000 0000 0002	Byte 5, bit 6	0x030000000040
Ring Error Monitor	0xC000 0000 0008	Byte 5, bit 4	0x030000000010
Configuration Report Server	0xC000 0000 0010	Byte 5, bit 3	0x030000000008
NetBIOS	0xC000 0000 0080	Byte 5, bit 0	0x030000000001
Bridge	0xC000 0000 0100	Byte 4, bit 7	0x030000008000
LAN Manager	0xC000 0000 2000	Byte 4, bit 2	0x030000000400
User-defined	0xC000 0008 0000 to 0xC000 4000 0000	Byte 3, bits 0-4; Byte 2, bits 1-7	0x030000100000 to 0x030002000000

Specifying VINES Address Ranges

You can obtain a VINES server address from a sniffer trace, or by converting the wfVinesIfEnry.wfVinesIfAdr entry (determined using the Technician Interface) from the decimal value to hexadecimal.

Example

If the address of a VINES server is **a2482c.0001**, enter the filter range as **0xa2482c0001**.

Specifying Source and Destination SAP Code Ranges

Table 5-3 lists some common SAP codes to use when specifying a range for Source or Destination SAP traffic filter criteria. The SAP code consists of a 7-bit SAP address and a 1-bit Command/Response field.

Table 5-3. SAP Codes

Description	SAP Code
XID or TEST *	00-01 *
Individual Sublayer Management	02
Group Sublayer Management	03
SNA	04-05, 08-09, 0C-0D
IP	06
Proway Network Management	0E
Novell and SDLC Link Servers	10
CLNP ISO OSI	20, 34, EC
BPDU	42
X.25 over 802.2 LLC2	7E
XNS	80
Nestar	86
Active station list	8E
ARP	98
SNAP	AA
Banyan VIP	BC
Novell IPX	E0
IBM NetBIOS	F0
LAN Network Manager	F4, F5
Remote Program Load	F8
IBM RPL	FC
ISO Network Layer	FE
LLC Broadcast	FF

*. The Command/Response bit makes the 0x00 byte look like 0x01.

Specifying Frame Relay NLPID Range Values

Table 5-4 lists several Frame Relay network layer protocol ID (NLPID) values you can use when specifying Frame Relay over IP traffic filter criteria.

Table 5-4. Frame Relay NLPID Values

Description	NLPID (0x)
IP	CC
OSI	81, 82, 83
SNAP	80

Specifying PPP Protocol ID Range Values

Table 5-5 lists some Data Link layer Protocol ID values you can use when specifying PPP over IP traffic filter criteria. Refer to RFC 1700 for a complete list.

Table 5-5. PPP Protocol ID Values

Description	Protocol ID (0x)
IP	0021
OSI	0023
Stream Protocol (ST2)	0033

Specifying TCP and UDP Port Range Values

Table 5-6 lists some common TCP port ranges you can use when specifying TCP over IP traffic filter criteria. .

Table 5-6. Source and Destination TCP Port Values

Description	TCP Port
FTP	20, 21
Telnet	23
SMTP	25

(continued)

Table 5-6. Source and Destination TCP Port Values *(continued)*

Description	TCP Port
DNS	53
Gopher	70
World Wide Web http	80 - 84
DLSw Read Port	2065
DLSw Write Port	2067

Table 5-7 lists common UDP port values.

Table 5-7. Source and Destination UDP Port Values

Description	UDP Port
DNS	53
TFTP	69
SNMP	161
SNMPTRAP	162

Specifying Ethernet Type Range Values

Table 5-8 lists some common Ethernet Type codes to use when specifying Ethertype criteria ranges. Refer to RFC 1700 for a complete and current list.

Table 5-8. Ethernet Type Codes

Description	Ethertype (0x)
Bay Networks Synchronous Pass-Through	80FF
Bay Networks Source Route Traffic (non-Token Ring media)	8101
Bay Networks Breath of Life Packet (BofL)	8102
Bay Networks Transparent Bridge Traffic on Token Ring	8103
Bridged Ethernet over RFC 1490 Frame Relay	0007
Bridged Token Ring over RFC 1490 Frame Relay	0009
Bridged FDDI over RFC 1490 Frame Relay	000A
Bridged PDUs over RFC 1490 Frame Relay	000B
802.3 Length Field	0000-05EE
802.5 Length Field	0000-05FF
Xerox PUP	0101-01FF, 0200, 0201
Nixdorf	0400
XNS (IDP)	0600
XNS (Address Translation)	0601
IP	0800
X.25	0801
CHAOSnet	0804
X.25 Level 3	0805
ARP	0806
XNS	0807
Symbolix	081C
Xyplex	0888-088A
UB Debugger	0900
XNS Address Translation	0A00-0A01
Banyan VINES	0BAD

(continued)

Table 5-8. Ethernet Type Codes *(continued)*

Description	Ethertype (0x)
DEC	6000-6009
DEC MOP	6001-6002
DRP	6003
DEC LAT	6004
LAVC	6007
3COM	6010-6014
UB Download	7000
UB NUI	7001
UB Boot Broadcast	7002
Proteon	7030
Cabletron	7034
Cronous	8003-8004
HP Probe	8005
Nestar	8006
Excelan	8010
Silicon Graphics	8013, 8014, 8015
HP Apollo Native Ethernet	8019
RARP	8035
DEC BPDU	8038
DEC	8039-8042
DEC Encryption	803D
DEC LAN Traffic Monitor	803F
DEC NetBIOS Emulator	8040
AT&T	8046-8047
Compugraphic	8069
Vitalink Management	807D-8080
Xyplex	8088-808A
Kinetics Ether-talk	809B
Spider	809F

(continued)

Table 5-8. Ethernet Type Codes *(continued)*

Description	Ethertype (0x)
Nixdorf	80A3
Siemens	80A4-80B3
Pacer Software	80C6
Applitek	80C7
Intergraph	80C8-80CC
Harris 3M	80CD-80CE
IBM SNA	80D5
Retix Bridge Management	80F2
AARP	80F3
Shiva	80F4
HP Apollo	80F7
Symbolics	8107-8109
Waterloo Software	8130
IPX over Frame Relay	8137
Novell	8137-8138
DEC MOP	9000
XNS Bridge Comm Management	9001
3Com	9002-9003

Specifying IP Codes

Table 5-9 lists some common Protocol and Type codes to use when specifying IP Type of Service and Protocol criteria ranges. Refer to RFC 1700 for a complete list.

Table 5-9. IP Type Codes

Description	Protocol/Type Code (decimal)
ICMP (Internet Control Message Packets)	1
IGP	9
RSVP (Reservation Protocol)	46
VINES	83
OSPF	89

Chapter 6
Applying Inbound Traffic Filters

This chapter shows how to use the Configuration Manager to configure inbound traffic filters. To complete the steps in this chapter you must first be familiar with protocol-specific filtering criteria and actions. Refer to Chapter 3 for this information.

Working with Inbound Traffic Filters

To apply traffic filters to a particular interface, you first use the Configuration Manager to display the Traffic Filters window for the configured protocol.

For all protocols *except* DLSw, you display the Traffic Filters window as described in the next section, "Displaying the Inbound Traffic Filters Window." For circuits configured with DLSw, go to the section "Displaying the DLSw Inbound Traffic Filters Window."

Once you display the protocol-specific Traffic Filters window, you can

- Create, copy, or edit a filter template ("Preparing Filter Templates")
- Apply a template to an interface ("Creating an Inbound Filter")
- Change an existing filter ("Editing an Inbound Filter")
- Change the filtering order ("Changing Filter Precedence")
- Temporarily disable or enable a filter ("Enabling or Disabling an Inbound Filter")
- Remove a filter from an interface ("Deleting an Inbound Filter")

Displaying the Inbound Traffic Filters Window

To display the inbound Traffic Filters window for all protocols except DLSw:

1. **Display the Configuration Manager window.**
2. **Select Circuits > Edit Circuits.**

   The Circuit List window appears (Figure 6-1).

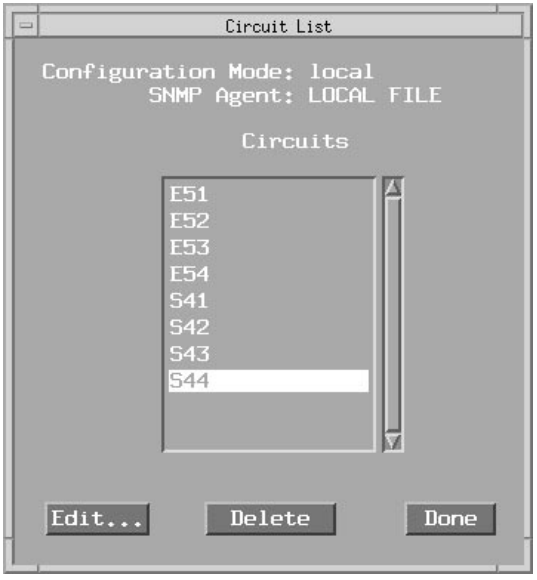

Figure 6-1. Circuit List Window

3. **Select the circuit to which you want to add a traffic filter.**
4. **Click on Edit.**

   The Circuit Definition window appears, with the circuit you selected highlighted (Figure 6-2).

5. **Select Protocols > Edit** *<protocol>* **> Traffic Filters.**

   The menu path to the Traffic Filters window is protocol-specific. Figure 6-2 shows the menu paths for a circuit configured with the Bridge protocol.

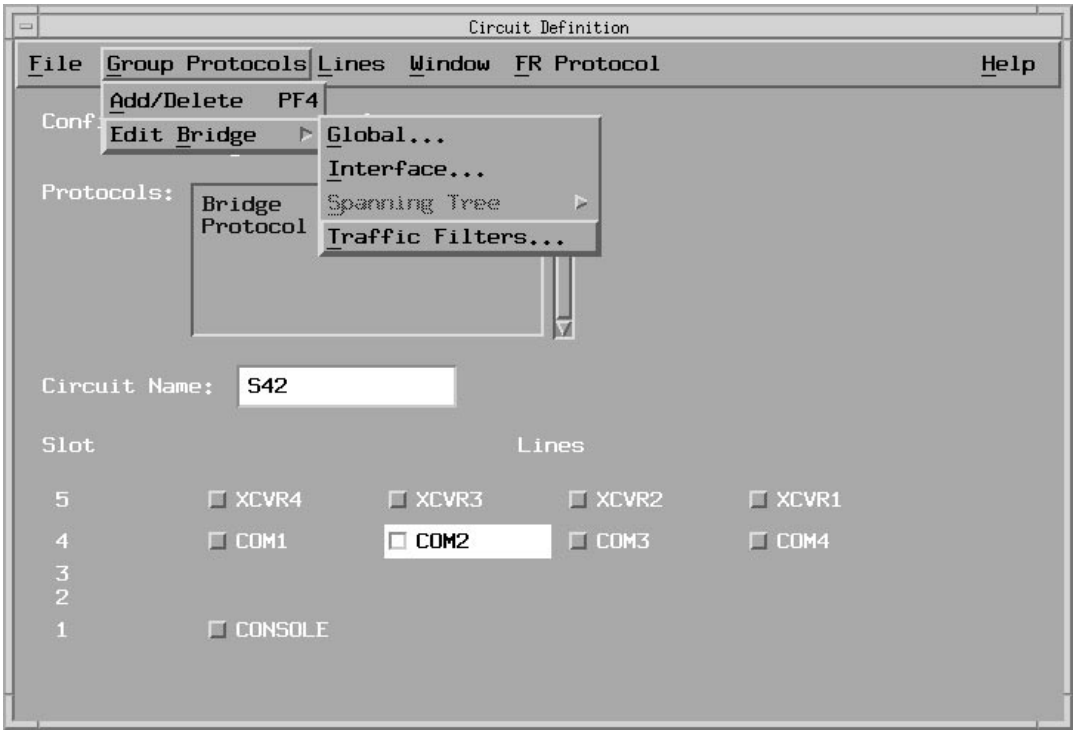

Figure 6-2. Selecting the Inbound Traffic Filters Menu (Bridge Example)

The Filters window for the selected circuit and protocol appears (Figure 6-4). Go to "Preparing Filter Templates."

Displaying the DLSw Inbound Traffic Filters Window

To display the DLS Traffic Filters window:

1. **Display the Configuration Manager window.**
2. **Select Protocols > DLSw > Traffic Filters (Inbound) (Figure 6-3).**

Figure 6-3. Selecting the DLSw Inbound Traffic Filters Window

The DLS Filters window appears. Although the Traffic Filters window is protocol-specific, you use the window the same way for all protocols. The examples in this chapter show the Bridge Filters window (Figure 6-4).

Preparing Filter Templates

This section describes how to add a filter template to an interface by

- Creating a New Template
- Customizing Templates

The section "Creating an Inbound Filter," later in this chapter, describes how to create a filter by applying (saving) a filter template to an interface.

Creating a New Template

To add a filter to an interface, you do not always need to create a new template. Often, you can begin with an existing template. If there is already a filter template for the circuit you are configuring that includes filter information you might use, go to "Customizing Templates."

If there is no existing template to match your needs, you must first create a new template for your circuit. To create a new template:

1. **Display the Filters window for your selected circuit (Figure 6-4 shows the Bridge Filters window).**

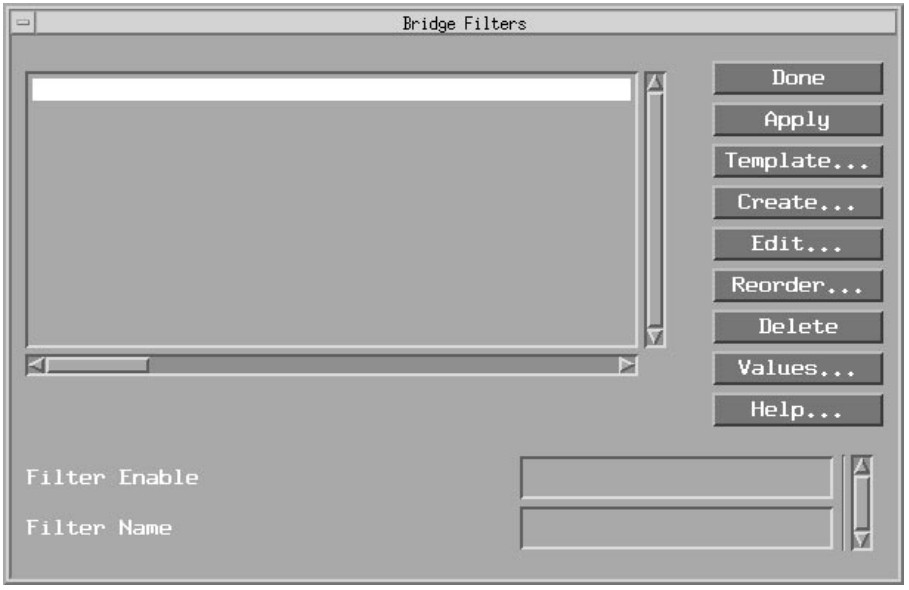

Figure 6-4. Inbound Traffic Filters Window

Note: Although the Traffic Filters menu is protocol-specific, you use the window the same way for all protocols.

2. **Click on Template.**

   The Filter Template Management window appears (Figure 6-5).

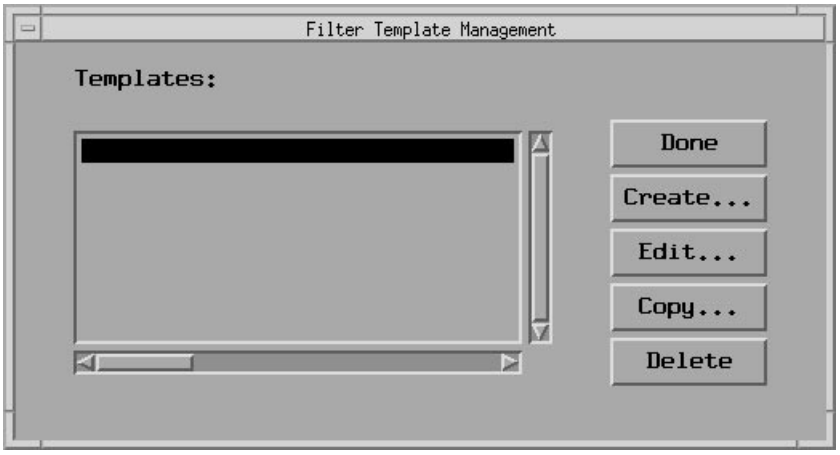

Figure 6-5. Filter Template Management Window

3. **Click on Create.**

   The Create Template window for your protocol appears (Figure 6-6).

Note: The Create Template window is protocol-specific. Figure 6-6 shows the Create Bridge Template window, but the window for other protocols is similar.

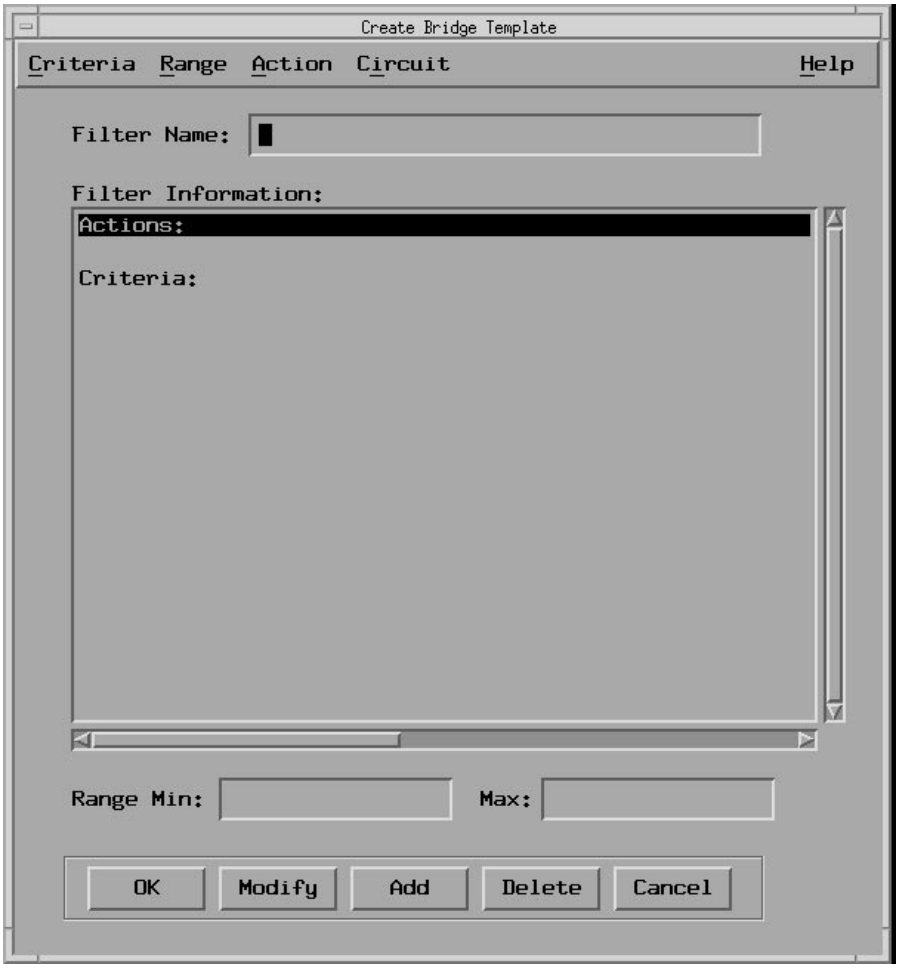

Figure 6-6. Create Template Window

4. **Enter a name for the new template in the Filter Name box.**

   Give descriptive names to your templates. For example, *Drop_Telnet* might be appropriate for a template that drops all locally initiated outbound Telnet sessions to remote nodes.

5. **Select Criteria > Add; then select the criterion that you want to use to filter packets (Figure 6-7).**

Each filter template can have only one criterion. Create new templates for additional criteria.

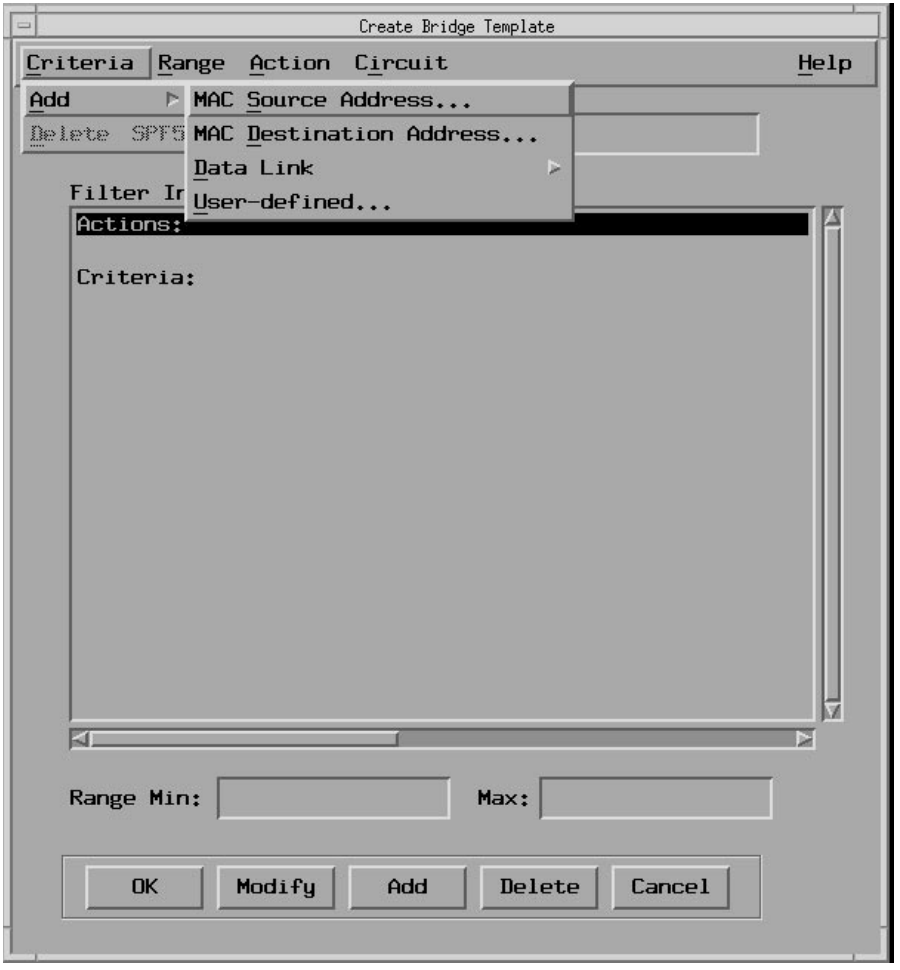

Figure 6-7. Selecting a Filter Criterion

The Add Range window appears (Figure 6-8). You must specify at least one range for each criterion.

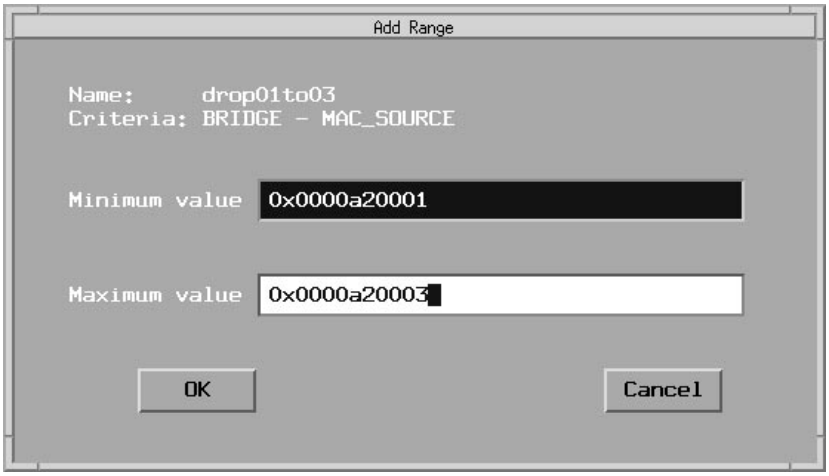

Figure 6-8. Add Range Window

6. **Specify the low and high values for the range you want to apply to the selected criterion.**

   In this example (refer to Figure 6-8), the range for the MAC source address criterion is from 0x0000A20001 (the minimum value) to 0x0000A200003 (the maximum value). Each incoming packet will be checked to see whether its MAC source address falls into this range of addresses.

   If the range you want to add consists of just one value, specify that value in both boxes.

Note: When you enter values for the Minimum and Maximum value parameters, the Configuration Manager assumes that the value is a decimal number. To enter a hexadecimal number, use the prefix 0x.

7. **Click on OK.**

   You return to the Create Filter Template window. The new criterion and range appear in the Filter Information scroll box (Figure 6-9).

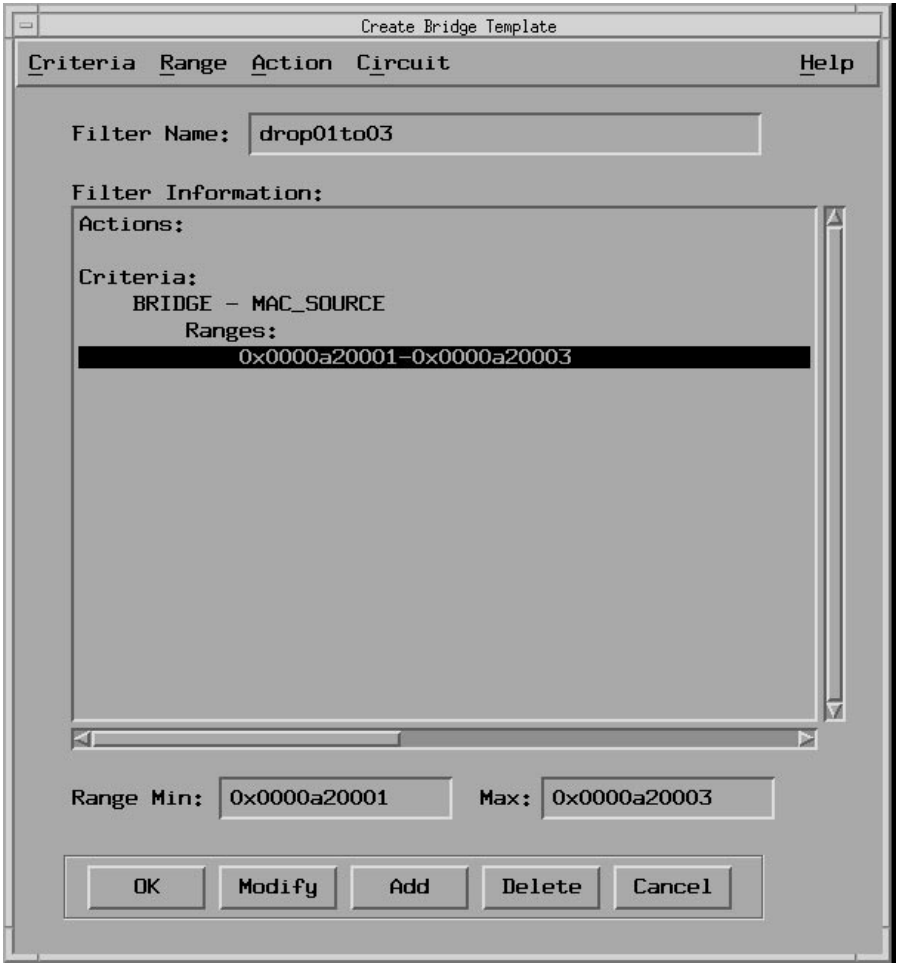

Figure 6-9. Create Template Window with Criteria and Range Added

8. **Add additional ranges if you want.**

   You can add up to 100 ranges for each filter criterion.

9. **Select Action > Add; then, select the action you want to impose on packets that match any of the template's ranges of filtering criteria.**

   The action is now associated with the new criterion and range which appear in the Filter Information scroll box (Figure 6-10).

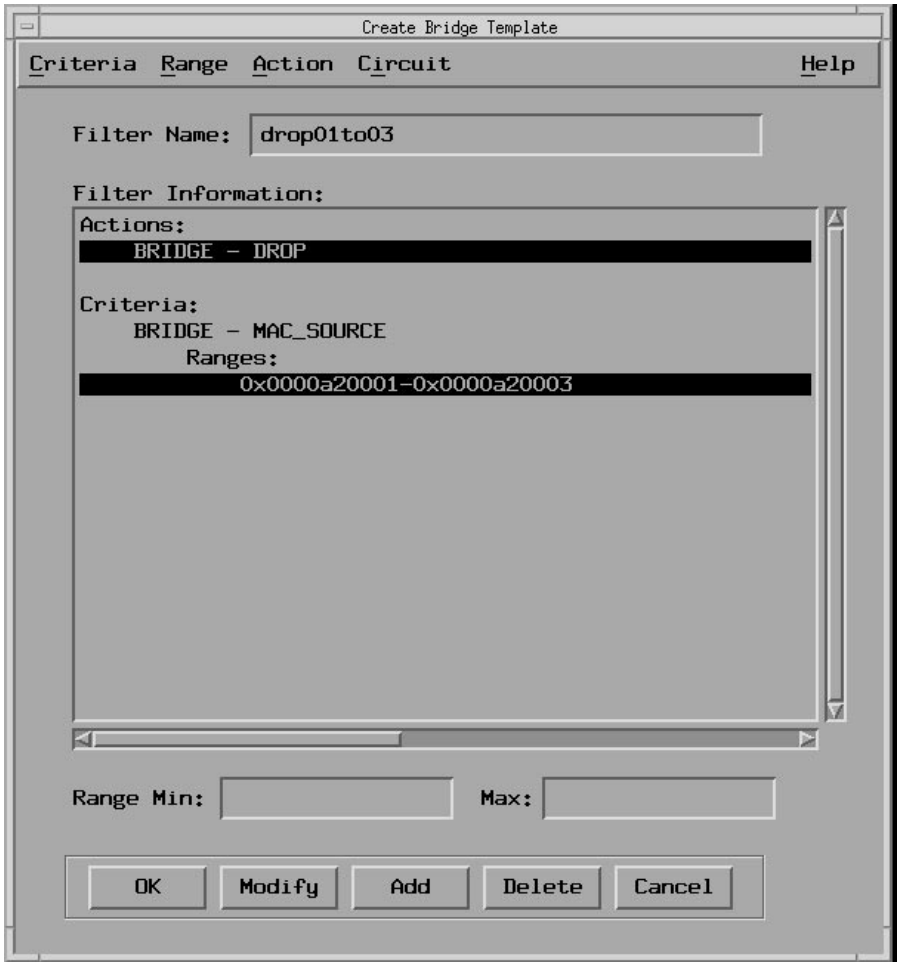

Figure 6-10. Actions List with New Action

10. **When you are finished adding actions to your template, click on OK.**

    You return to the Filter Template Management window (refer to Figure 6-5).

Customizing Templates

There are two ways to change a filter template:

- Copy the existing template, rename it, and then edit it.

  This preserves the original template and creates an entirely new template with the same criteria and actions. You can then modify the new version to suit your needs.

- Edit the existing template.

  If you do not want or need to preserve the original template, you can edit it without first copying and renaming it. (Changing a template does not affect interfaces to which the template has already been applied.)

To edit an existing template without preserving the original, go to "Editing a Template."

Copying a Template

To duplicate an existing template:

1. **Display the Filter Template Management window (refer to Figure 6-5).**
2. **Select a template from the scroll box.**
3. **Click on Copy.**

   The Copy Filter Template window appears (Figure 6-11).

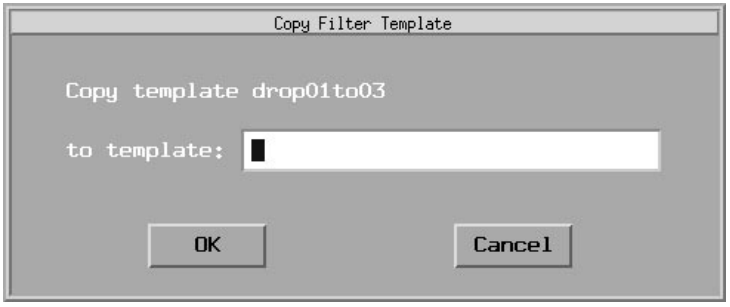

Figure 6-11. Copy Filter Template Window

4. **Enter a name for the new template in the box provided.**

   Remember that it is a good idea to give your template a name that reflects its contents.

5. **Click on OK.**

   You are returned to the Filter Template Management window. The name you just assigned to the new template appears in the Templates box.

Editing a Template

After you create or copy a template, you can edit it to apply the filters you want.

1. **Display the Filter Template Management window (Figure 6-5).**
2. **Select the template you want to edit from the scroll box.**
3. **Click on Edit.**

   The Edit Filter Template window appears. As in the Create Filter Template window (refer to Figure 6-9), you can add or delete filter criteria, ranges, and actions, as described in Table 6-1.

4. **Click on OK when you are finished editing the template.**

   You return to the Filter Template Management window. You can continue to create, edit, or delete templates using this window.

5. **Click on Done to return to the Inbound Traffic Filters window (refer to Figure 6-4).**

Table 6-1. Using the Edit Filter Template Window

Task	Site Manager Instructions	Notes
Add a criterion	1. Select Criteria > Add; then select the criterion to use to filter packets. 2. Add a range in the Add Range window.	For any criterion you choose, you must specify at least one range. Each template can have only one criterion.
Delete a criterion	1. Select the criterion to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Criteria window.	Each filter template has only one criterion. Create new templates for additional criteria.
Add a range	1. Select the criterion in the Filter Information box. 2. Click on Add. 3. Use the Range Min and Max boxes to specify low and high values for the range.	Ranges are listed beneath a criteria in the Filter information scroll box. You can add up to 100 ranges for each filter criterion.
Modify a range	1. Select the range to modify in the Filter Information box. 2. Click on Modify. 3. Use the Range Min and Max boxes to specify new low and high values for the range.	When entering range values, you must use the prefix 0x to specify a hexadecimal number.
Delete a range	1. Select the range to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Range window.	You must have at least one range specified for each criterion.
Add an Action	1. Select Action > Add in the Edit Filters window; then select the action to impose on packets that match any of the template's ranges of filtering criteria. 2. When you are finished adding actions to your template, click on OK.	With the exception of the Log action, each filter template has only one action. You can select Log in combination with any other action. Create new templates for additional actions.
Delete an Action	1. In the Filter Information scroll box, select the action you want to remove. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Action window.	There must be one at least action specified for a filter template.

Creating an Inbound Filter

You create an inbound traffic filter by applying a filter template to an interface.

Note: Try to create the filters on each interface in order of precedence. The first filter you create has the highest precedence and a rule number of 1. Subsequent filters created on the interface have decreasing precedence. See “Changing Filter Precedence” for information on filter precedence.

To create an inbound traffic filter:

1. **Display the Inbound Filters window for your selected circuit and protocol.**

   See the first section of this chapter, “Working with Inbound Traffic Filters.”

2. **Click on Create Filter.**

   The Create Filter window appears (Figure 6-12).

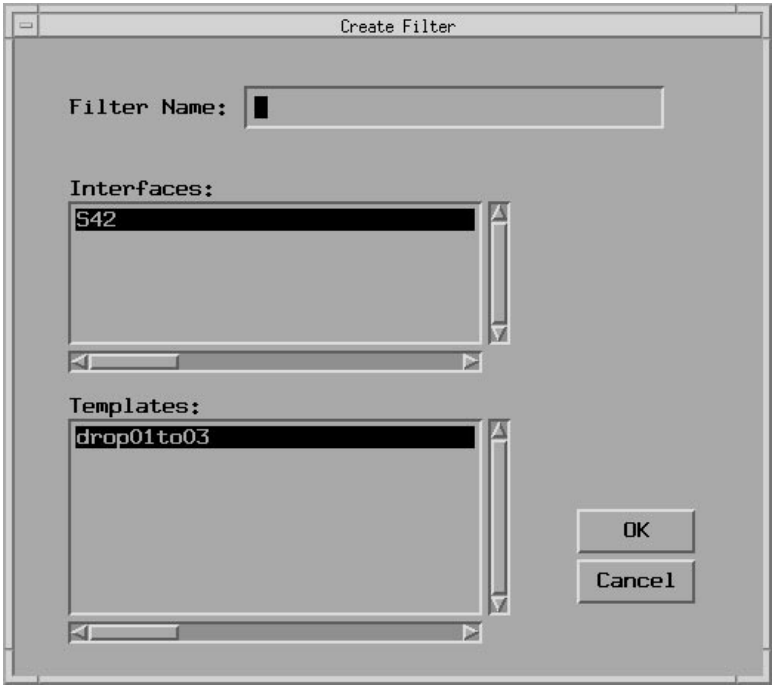

Figure 6-12. Create Filter Window

3. **Verify the name of the selected interface.**
4. **Select the appropriate template in the Templates scroll box.**
5. **In the Filter Name field, enter a meaningful name for the new filter.**

   It can be helpful to includes the circuit name. For example, *Drop_Telnet_E21*.

Note: The name of the filter can be the same name as the template.

6. **Click on OK.**

   You are returned to the Traffic Filters window (Figure 6-13).

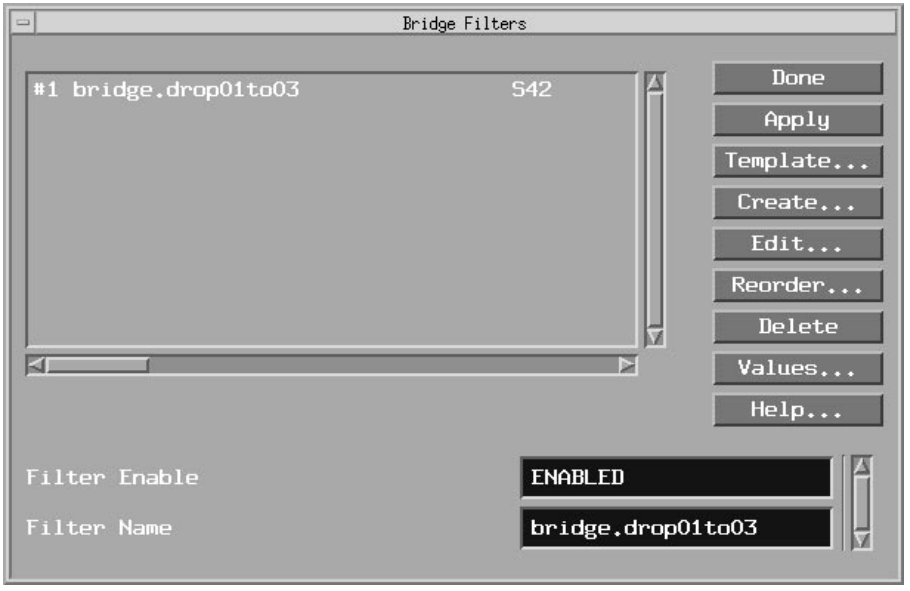

Figure 6-13. New Filter Listed in the Filters Window Scroll Box

In Figure 6-13, the filter named *bridge.drop01to03* consists of the template selected in Figure 6-12 applied to interface S42.

Editing an Inbound Filter

After you apply a filter to an interface, you can edit its criteria, ranges, and actions. If you used a template edited to suit your needs, you probably don't need to make further edits.

To customize a specific filter, you have the following options:

- Add or delete filtering criteria
- Add, modify, or delete criteria ranges
- Add or delete actions

To customize an inbound filter:

1. **Display the Filters window for the circuit you are editing (Figure 6-13).**
2. **In the scroll box, click on the name of the filter you want to edit.**
3. **Click on Edit.**

   The Edit Filters window for your protocol appears; Figure 6-14 shows the Edit Bridge Filters window.

Note: The Edit Filters window is protocol-specific. Figure 6-14 shows the Edit Bridge Filters window; the window for other protocols is similar.

---

4. **Use the Edit Filters window to add, change, or delete filter criteria, ranges, and actions as described in Table 6-2.**

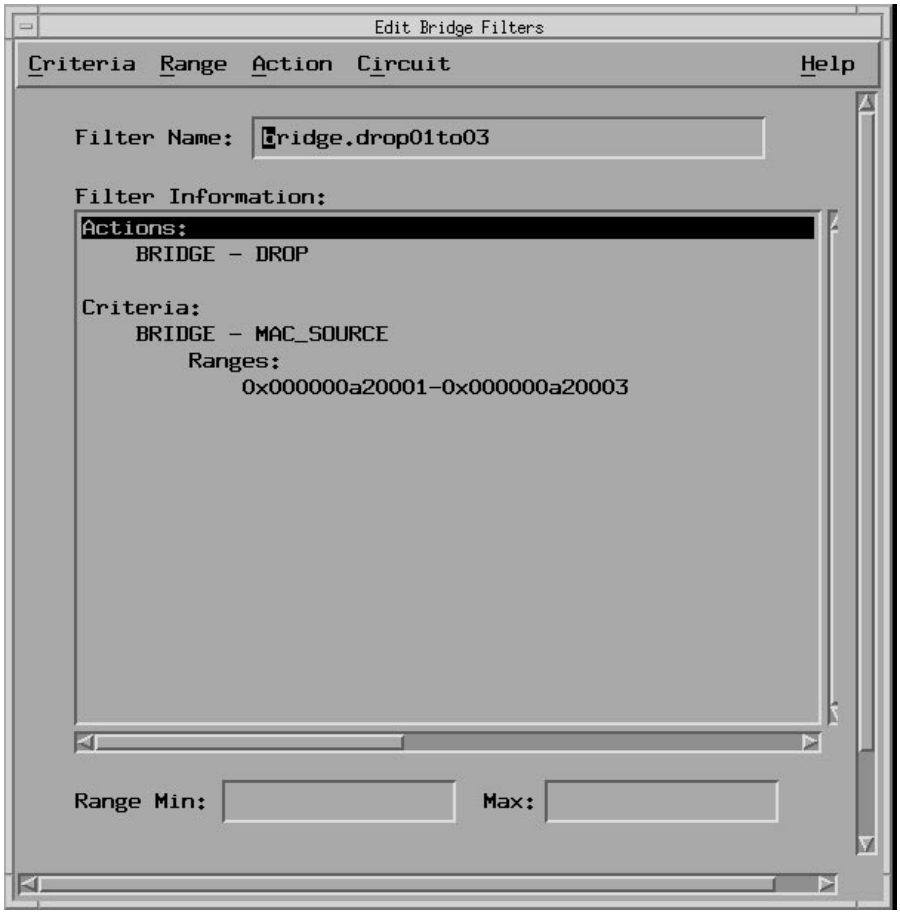

Figure 6-14. Edit Filters Window

Table 6-2. Using the Edit Filters Window

Task	Site Manager Instructions	Notes
Add a criterion	1. Select Criteria > Add; then select the criterion to use to filter packets. 2. Add a range in the Add Range window.	For any criterion you choose, you must specify at least one range. Each template can have only one criterion.
Delete a criterion	1. Select the criterion to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Criteria window.	Each filter template has only one criterion. Create new templates for additional criteria.
Add a range	1. Select the criterion in the Filter Information box. 2. Click on Add. 3. Use the Range Min and Max boxes to specify low and high values for the range.	Ranges are listed beneath a criteria in the Filter information scroll box. You can add up to 100 ranges for each filter criterion.
Modify a range	1. Select the range to modify in the Filter Information box. 2. Click on Modify. 3. Use the Range Min and Max boxes to specify new low and high values for the range.	When entering range values, you must use the prefix 0x to specify a hexadecimal number.
Delete a range	1. Select the range to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Range window.	You must have at least one range specified for each criterion.
Add an Action	1. Select Action > Add in the Edit Filters window; then select the action to impose on packets that match any of the template's ranges of filtering criteria. 2. When you are finished adding actions to your template, click on OK.	With the exception of the Log action, each filter template has only one action. You can select Log in combination with any other action. Create new templates for additional actions.
Delete an Action	1. In the Filter Information scroll box, select the action to remove. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Action window.	There must be one at least action specified for a filter template.

Specifying User-Defined Criteria

In addition to predefined criteria, the Edit Filters and Create Filter Template windows provide a “User-Defined” criterion choice for most protocols. The User-Defined option allows you to set up filtering criteria based on bit patterns within a packet’s header that are not supported in predefined criteria.

Setting up user-defined criteria is similar to using up predefined criteria, except you must specify the criterion’s location within the packet. (With predefined criteria, the locations are established.) Refer to Chapter 3 for the supported protocol header reference points you can use to specify user-defined traffic filter criteria.

To specify user-defined criteria:

1. **In the Edit Filters or Create Filter Template window, select the User-Defined option from the Criteria menu.**

   The Add User-Defined Field window appears (Figure 6-15). In this window, you specify the criterion’s location.

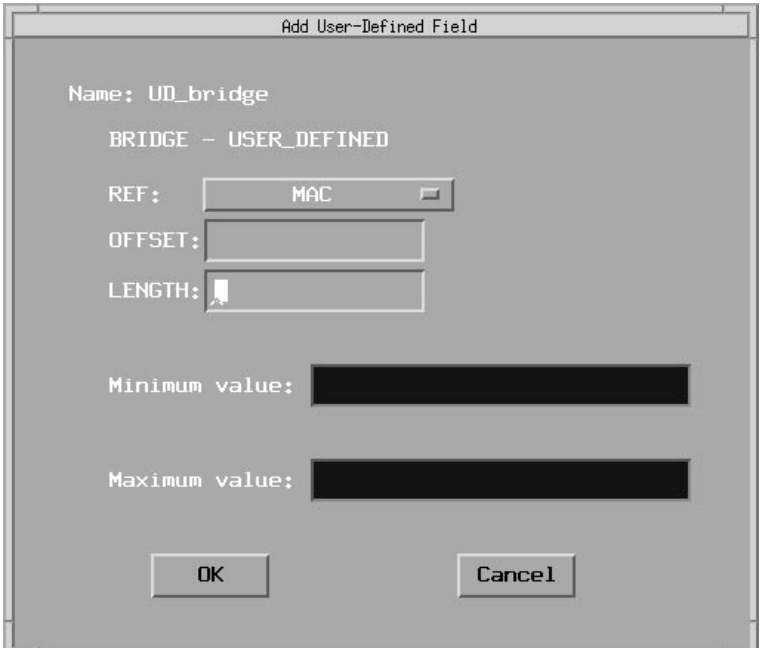

Figure 6-15. Add User-Defined Field Window

2. **Select the protocol-specific reference field.**

   In this example, the choices are the MAC or Data Link header.

3. **Specify an offset and length from the reference field.**

4. **Specify a range associated with the bit criterion described by the reference, offset, and length (Figure 6-16).**

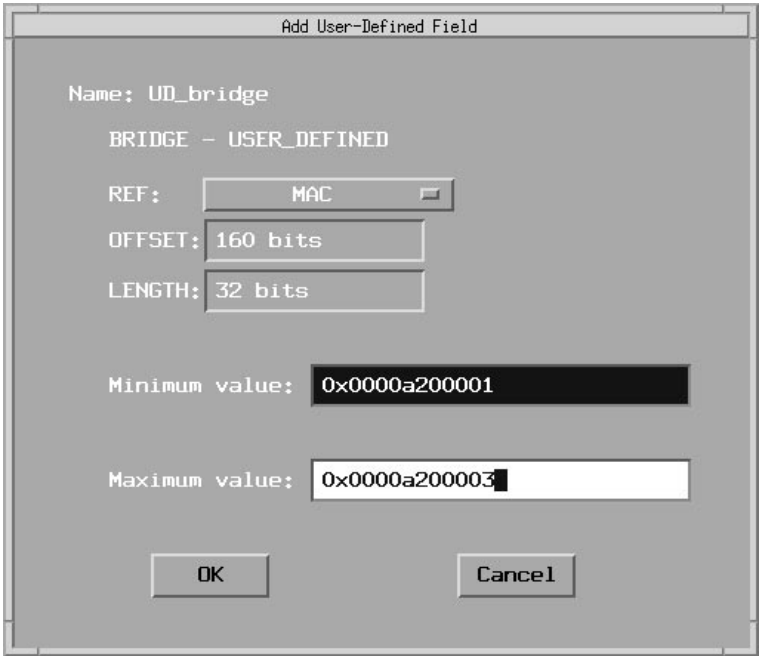

Figure 6-16. User-Defined Criteria

5. **Click on OK.**

The procedures in this chapter for adding, deleting, and editing ranges for predefined criteria can be used for a user-defined criterion as well.

Changing Filter Precedence

You can assign as many as 31 inbound traffic filters per protocol to each router interface. As you add filters to an interface, the Configuration Manager numbers them chronologically (#1, #2, #3, and so on -- as seen in Figure 6-17). The number determines the filter precedence; lower filter numbers have higher precedence.

If a packet matches two filters, the filter with the highest precedence (lowest number) applies. For example, if the first filter on the interface (Filter No. 1) accepts a packet and the second filter (Filter No. 2) drops the same packet, Filter No. 1 has precedence and the packet will be accepted.

Figure 6-17 shows how the Traffic Filters window displays the filters on an interface. The first filter created has the highest precedence and the number 1.

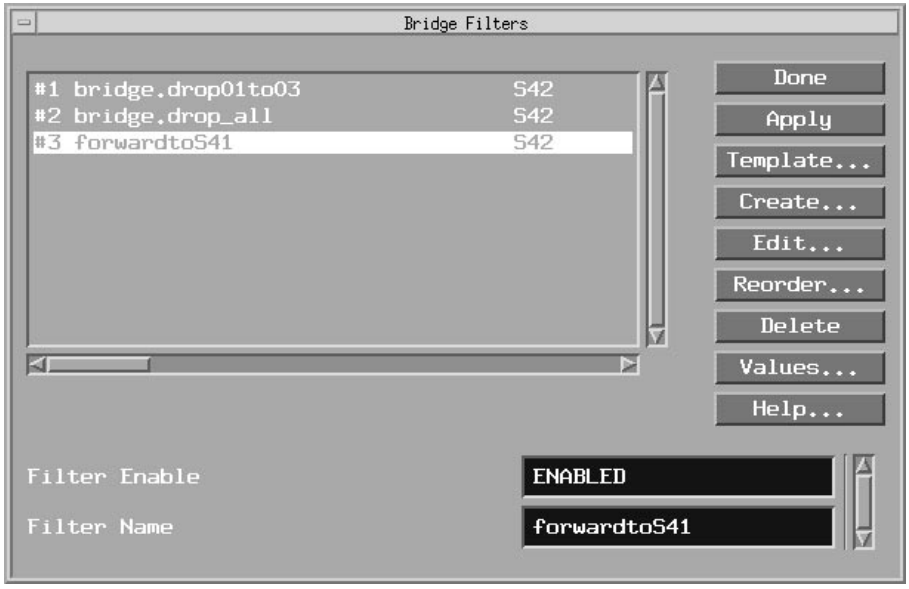

Figure 6-17. Traffic Filters List (in Order Created)

Try to create filters on an interface in order of precedence. However, if you can't, or if your filtering strategy changes, you can use the Traffic Filters window to rearrange the precedence of existing filters.

To change the order of precedence:

1. **In the Traffic Filters window, select the filter whose precedence you want to change.**
2. **Click on Reorder.**

   The Change Precedence window appears (Figure 6-18).

Figure 6-18. Change Precedence Window

3. **Click on either INSERT BEFORE or INSERT AFTER; then, type a filter rule number in the Precedence Number box.**

   The selected filter will now have a filter number that is either one higher (if you chose INSERT BEFORE) or one lower (if you chose INSERT AFTER) than the number you entered.

   For the example shown in Figure 6-19, if you wish to place the selected filter *before* #1, click on INSERT BEFORE and type **1** in the Precedence Number box.

Note: When reversing the order of the second-to-lowest and lowest precedence filters, the filter you select with the Reorder button and the filter number you specify in the Precedence Number box are the same. For example: to put Filter No. 2 at the bottom of a list of three filters (#1, #2, and #3), select Filter No. 2 and specify INSERT AFTER, Precedence Number: 2.

4. **Click on OK.**

You are returned to the Filters window. The filters now appear in their new order of precedence (Figure 6-19).

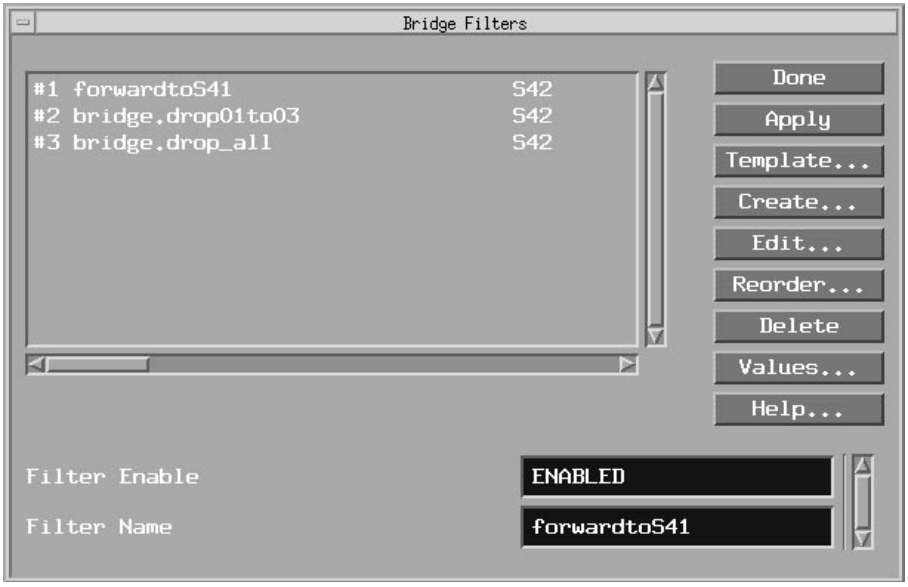

Figure 6-19. Traffic Filters List (Reordered Precedence)

Enabling or Disabling an Inbound Filter

Instead of deleting a filter from a circuit, you may want to turn off the filter temporarily. You can do this by disabling the filter on a circuit. Later, you can re-enable the filter.

To disable (or re-enable) a filter:

1. **Display the Traffic Filters window for your protocol (Figure 6-20).**

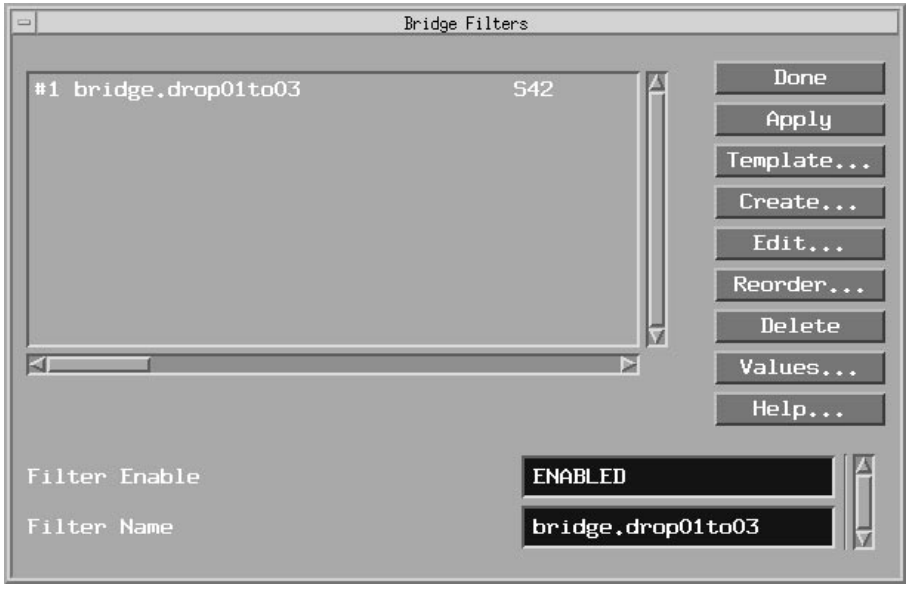

Figure 6-20. Traffic Filters Window

2. **Select the filter that you want to disable or re-enable in the filter scroll box.**
3. **Click on Values.**

   The Values Selection window appears.
4. **To disable a filter, change the value in the Filter Enable box from Enabled to Disabled.**

   To re-enable the filter, change the value in the Filter Enable parameter box from Disabled to Enabled.
5. **Click on OK.**

   You return to the Traffic Filters window.
6. **Click on Apply to save this change.**

Deleting an Inbound Filter

When you delete a filter, it affects only the interface from which the filter is removed.

To delete a filter from an interface:

1. **Display the Traffic Filters window (see Figure 6-20).**
2. **Select the filter that you want to delete in the scroll box.**

Caution: There is no confirmation of a filter deletion. Be sure to select a filter that you are certain you want to delete.

3. **Click on Delete.**

   The filter no longer appears in the scroll box of the Filters window.
4. **Click on Apply to save this change.**

Chapter 7
Applying Outbound Traffic Filters

This chapter shows how to use the Configuration Manager to configure outbound traffic filters.

You implement protocol prioritization by applying an outbound filter that includes a queue action (also called *priority filter*s). For instructions on how to edit edit the protocol prioritization parameters, refer to Chapter 2.

Note: To complete the steps in this chapter, you must be familiar with protocol-specific filtering criteria and actions. Refer to Chapter 4 for this information.

Working with Outbound Traffic Filters

To configure outbound traffic filters, you first display the Configuration Manager Priority/Outbound Filters window, as described in the next section. From the Priority/Outbound Filters window you can

- Create, copy, or edit a filter template (“Preparing Filter Templates”)
- Apply a filter template to an interface (“Creating an Outbound Filter”)
- Change an existing filter (“Editing an Outbound Filter”)
- Change the filtering order (“Changing Filter Precedence”)
- Temporarily disable or enable a filter (“Enabling or Disabling an Outbound Filter”)
- Remove a filter from an interface (“Deleting an Outbound Filter”)

Displaying the Priority/Outbound Filters Window

To configure outbound traffic filters for a particular interface, you must first display the Priority/Outbound Filters window for the circuit's protocol.

Note: For information about using the outbound traffic filters window for an interface configured with DLSw, see *Configuring DLSw Services*.

Complete the following steps to display the Priority/Outbound Filters window, enabling protocol priority if necessary.

1. **In the Configuration Manager window, click on a circuit interface connector. .**

   For Ethernet, FDDI, HSSI, Synchronous, or Token Ring interfaces, a popup menu appears.

   For MCE1 or MCT1 interfaces, the Logical Lines window appears.

2. **Click on Edit Circuit (for MCE1/MCT1, click on Circuit).**

   The Circuit Definition window appears (Figure 7-1). If Protocol Priority appears in the Protocols scroll box, go to Step 6.

Note: On circuits configured with Frame Relay or PPP, protocol prioritization is enabled by default. Otherwise, you must enable Protocol Priority the first time you configure outbound traffic filters.

3. **Select Protocols** > **Add/Delete.**

   The Select Protocols window appears.

4. **Select Protocol Priority from the list of protocols.**

   The Protocol Priority option is located near the end of the list.

5. **Click on OK.**

   The Circuit Definition window reappears.

6. **Select Protocols** > **Edit Protocol Priority** > **Priority/Outbound Filters (Figure 7-1).**

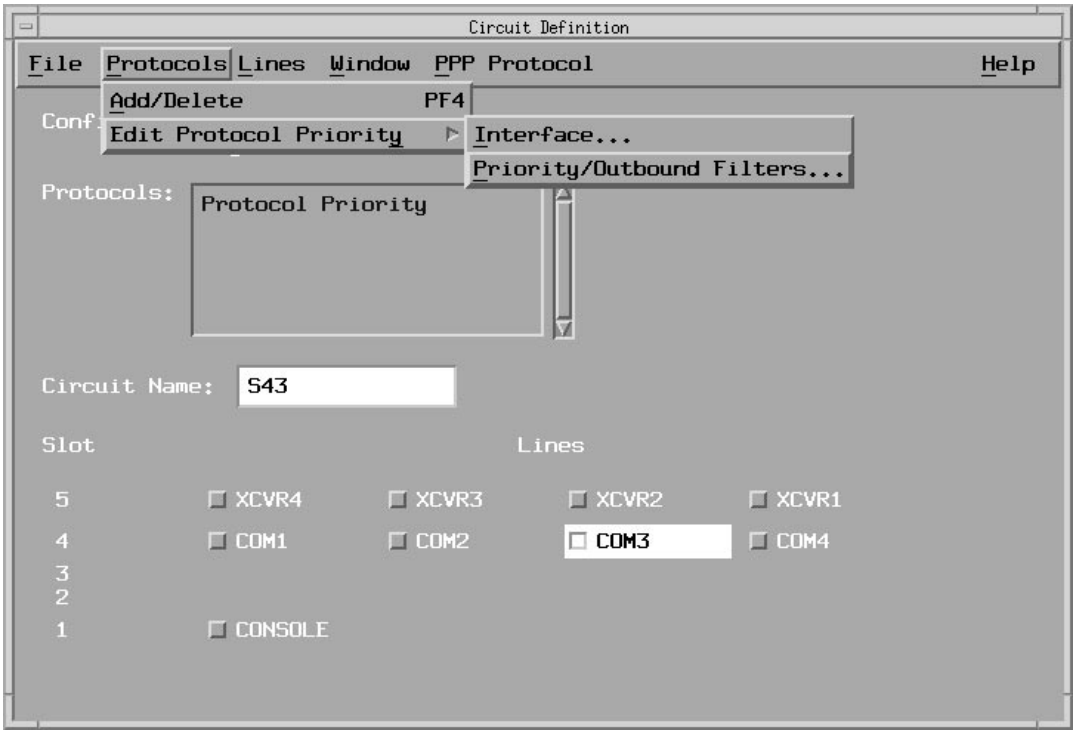

Figure 7-1. Selecting the Priority/Outbound Filters Window

The Priority/Outbound Filters window appears.

Preparing Filter Templates

This section describes how to add a filter template to an interface by

- Creating a new filter template or using an existing template
- Adding filtering criteria, ranges, and actions to a template
- Modifying and deleting templates

Note: Changing a template does not affect interfaces to which the template has already been applied.

The section "Creating an Outbound Filter," later in this chapter, describes how to create a filter by applying (saving) a filter template to an interface.

Creating a New Template

To add a filter to an interface, you do not always need to create a new template. Often, you can begin with an existing template. If there is already a filter template for the circuit you are configuring that includes filter information you might use, go to "Customizing Templates" or "Creating an Outbound Filter."

If there is no existing template to match your needs, you must first create a new template for the circuit. To create a new template from scratch:

1. **Display the Priority/Outbound Filters window (Figure 7-2).**

   See the previous section, "Displaying the Priority/Outbound Filters Window" for instructions.

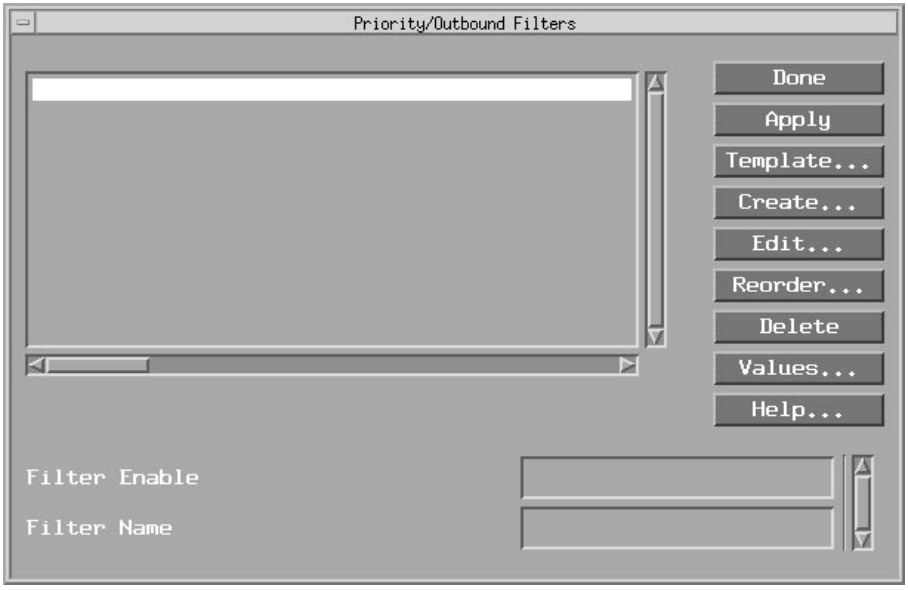

Figure 7-2. Priority/Outbound Filters Window

2. **Click on Template.**

   The Filter Template Management window appears (Figure 7-3).

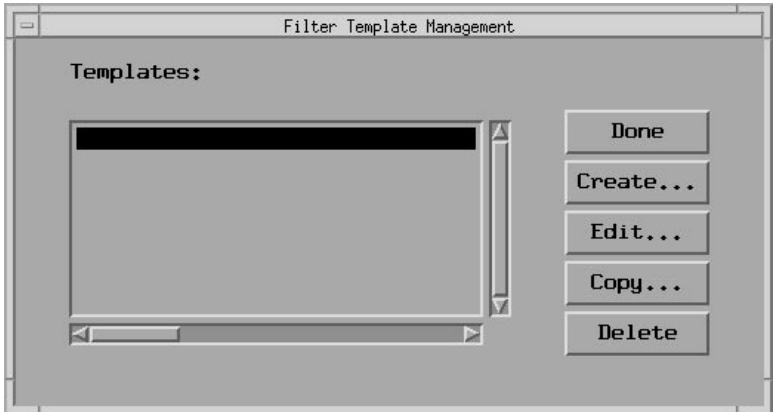

Figure 7-3. Filter Template Management Window

3. Click on Create.

The Create Priority/Outbound Template window appears.

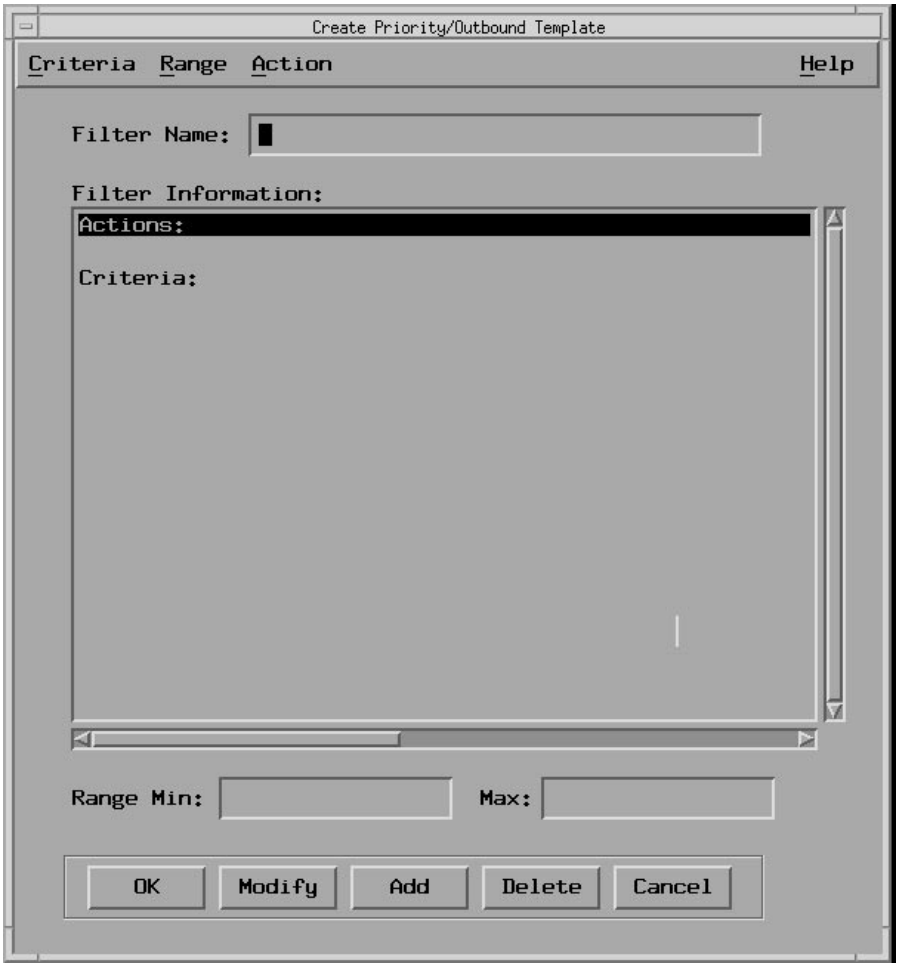

Figure 7-4. Create Priority/Outbound Template Window

4. **Enter a descriptive name for the template in the Filter Name box.**

   For instance, the name *Bridge01to03* might be appropriate for a template that contains information for filtering bridge frames from MAC source addresses 0x0000A2000001 to 0x0000A2000003.

5. **Select Criteria > Add; then select either Datalink or IP (Figure 7-5).**

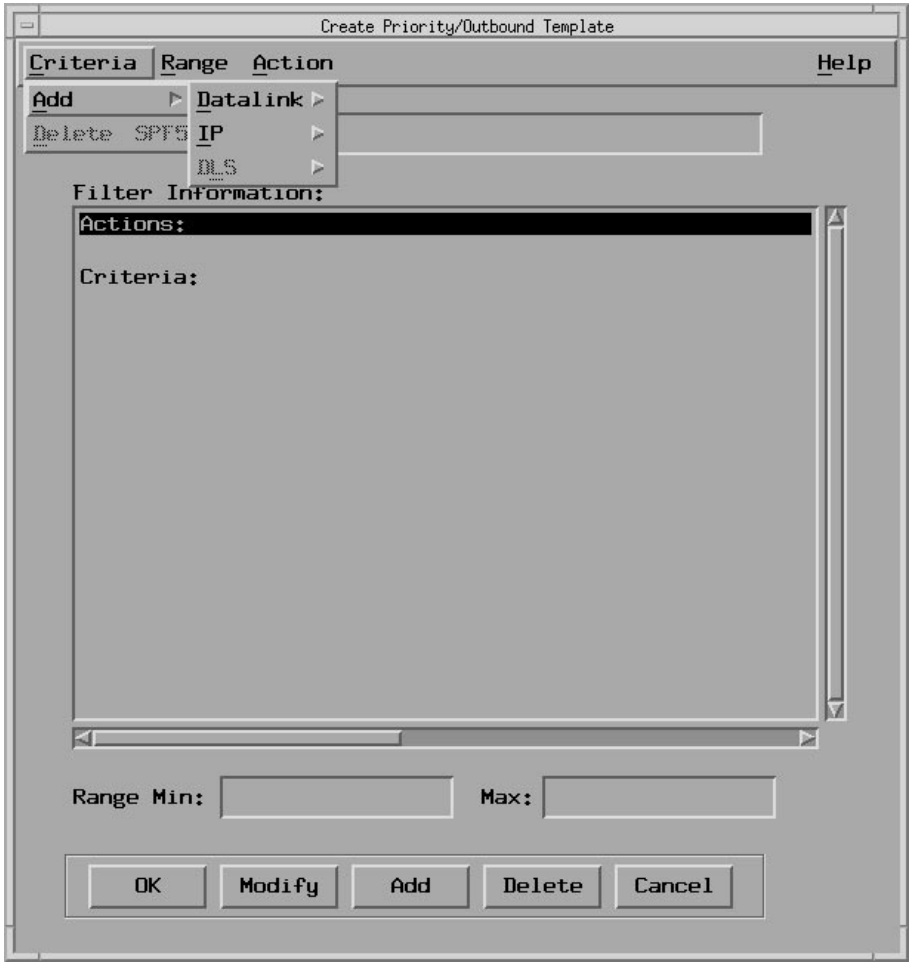

Figure 7-5. Selecting Outbound Traffic Filter Criteria

6. **Select the protocol-specific criterion you to add.**

   Each filter template can have only one criterion. Create new templates for additional criteria. Refer to Chapter 4 for information about the outbound traffic filter criteria for your selected interface.

   The Add Range window appears (Figure 7-6). You must specify at least one range value for each criterion.

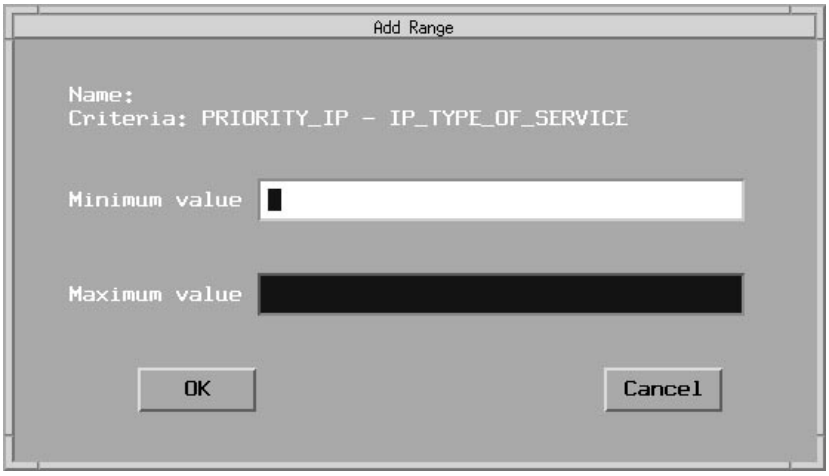

Figure 7-6. Add Range Window

7. **Specify the low and high values for the range you to apply to the selected criterion.**

   If the range you want consists of just one value, specify that value in both boxes. Zero is not a valid entry for Minimum or Maximum value.

Note: When you enter values for the Minimum and Maximum value paramters, the Configuration Manager assumes the value is a decimal number. To enter a hexadecimal number, use the prefix 0x.

8. **Click on OK.**

   The Create Priority/Outbound Template window reappears (refer to Figure 7-5). The new criterion and range appear in the Filter Information scroll box.

9. **Add additional ranges if you want.**

   You can add up to 100 ranges for each filter criterion.

10. **Select Action, and either IP or Datalink.**

11. **Select Add Action; then select the action you to impose on packets that match any of this template's ranges of filtering criteria.**

If you selected the Length action, go to “Specifying Prioritization Length.” For other actions, the Create Priority/Outbound Template window appears, showing the newly selected criteria, range, and action in the Filter Information scroll box (Figure 7-7).

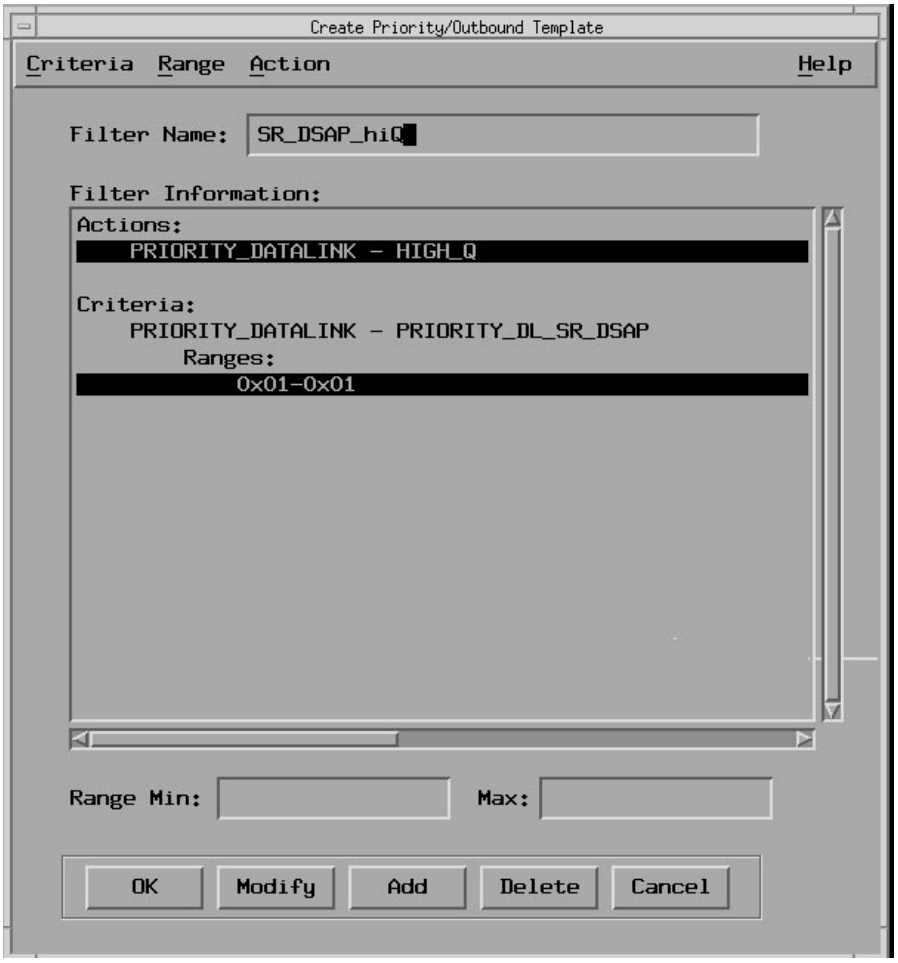

Figure 7-7. Create Priority/Outbound Template Window with Criteria and Actions

12. **When you are finished adding actions to your template, click on OK.**

    You return to the Filter Template Management window (refer to Figure 7-3).

Specifying Prioritization Length

If you select the Length action in the Create Priority/Outbound Template window, the Prioritization Length window (Figure 7-8) appears.

The Length action directs the router to place packets into a priority queue, based on a specified byte length. The packet length determines which queue.

Figure 7-8. Prioritization Length Window

1. **In the Prioritization Length window, edit the Packet Length.**

   Enter a packet length value between 0 and 4608 bytes to define a packet length measurement to which each packet is compared. An action is imposed on every packet, depending on whether it is less than, equal to, or greater than the value you set for this parameter. This action also depends on the values of the Less Than or Equal Queue and the Greater Than Queue parameters.

2. **In the Prioritization Length window, edit theLess Than or Equal Queue**

   Specify High, Low, or Normal as the queue a packet is placed in if its packet length is less than or equal to the value of the Packet Length parameter.

   For example, if Packet Length is set to 1024 bytes, any packet that is 1024 bytes or smaller is placed in the queue you choose for this parameter.

3. **In the Prioritization Length window, edit the Greater Than Queue**

Specify High, Low, or Normal as the queue a packet is placed in if its packet length is greater than the value of the Packet Length parameter.

For example, if Packet Length is set to 1024 bytes, any packet that is 1025 bytes or larger is placed in the queue you choose for this parameter.

4. **Click on OK.**

   The Create Priority/Outbound Template window appears, showing the newly selected criteria, range, and action in the Filter Information scroll box (refer to Figure 7-7).

Customizing Templates

There are two ways to change a filter template:

- Copy the existing template, rename it, and then edit it.

  This preserves the original template and creates an entirely new template with the same criteria and actions. You can then modify the new version to suit your needs.

- Edit the existing template.

  If you do not want or need to preserve the original template, you can edit it without first copying and renaming it. (Changing a template does not affect interfaces to which the template has already been applied.)

To edit an existing template without preserving the original, go to "Editing a Template."

Note: You can also edit or copy a template using a text editor. The Configuration Manager stores all templates in a file called template.flt.

Copying a Template

To duplicate an existing template:

1. **Display the Filter Template Management window (refer to Figure 7-3).**
2. **Select a template from the scroll box.**
3. **Click on Copy.**

   The Copy Filter Template window appears (Figure 7-9).

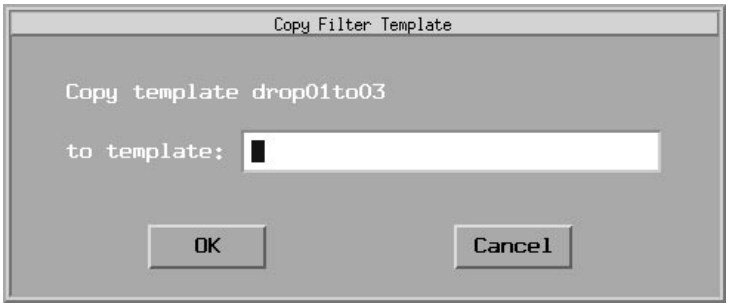

Figure 7-9. Copy Filter Template Window

4. **Enter a name for the new template in the box provided.**

   Remember that it is a good idea to give your template a name that reflects its contents.

5. **Click on OK.**

   You are returned to the Filter Template Management window. The name you just assigned to the new template appears in the Templates box.

Editing a Template

After you create or copy a template, you can edit it to apply the filters you want.

1. **Display the Filter Template Management window.**
2. **Select the template you to edit from the scroll box.**
3. **Click on Edit.**

   The Edit Priority/Outbound Template window window appears (Figure 7-10).

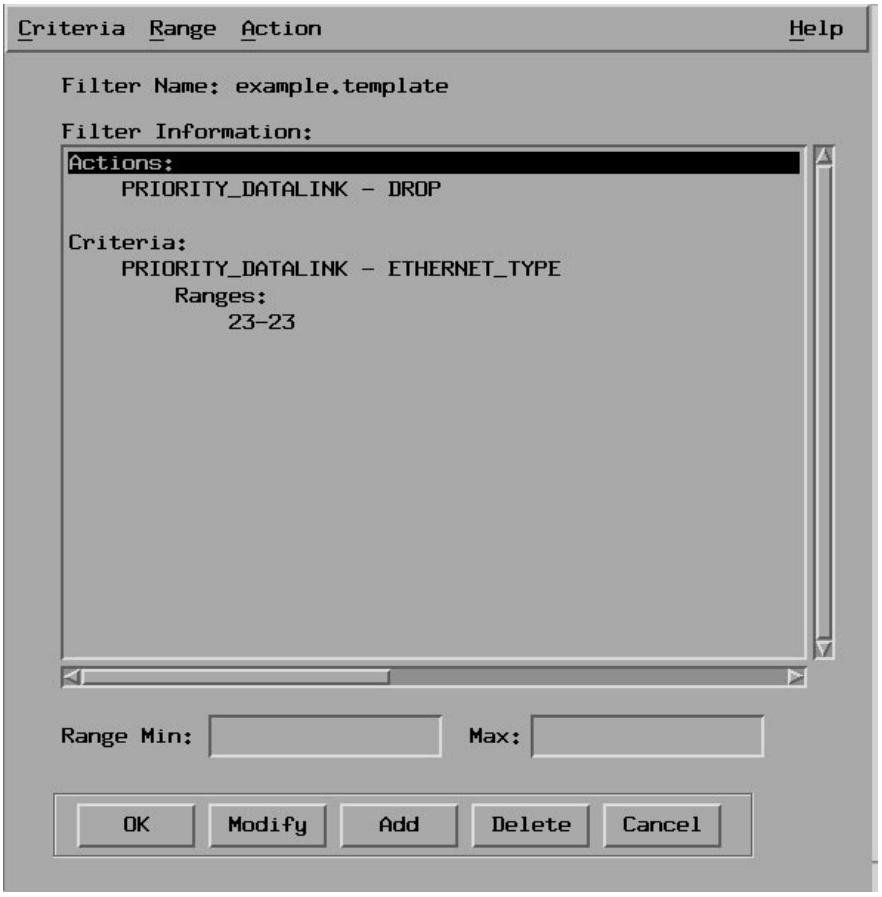

Figure 7-10. Edit Priority/Outbound Template Window

You can add or delete filter criteria, ranges, and actions in the Edit Priority/Outbound Template window as described in Table 7-1.

Table 7-1. Using the Edit Priority/Outbound Filter Template Window

Task	Site Manager Instructions	Notes
Add a criterion	1. Select Criteria > Add; then select the criterion to use to filter packets. 2. Add a range in the Add Range window.	For any criterion you choose, you must specify at least one range. Each template can have only one criterion.
Delete a criterion	1. Select the criterion to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Criteria window.	Each filter template has only one criterion. Create new templates for additional criteria.
Add a range	1. Select the criterion in the Filter Information box. 2. Click on Add. 3. Use the Range Min and Max boxes to specify low and high values for the range.	Ranges are listed beneath a criteria in the Filter information scroll box. You can add up to 100 ranges for each filter criterion.
Modify a range	1. Select the range to modify in the Filter Information box. 2. Click on Modify. 3. Use the Range Min and Max boxes to specify new low and high values for the range.	When entering range values, you must use the prefix 0x to specify a hexadecimal number.
Delete a range	1. Select the range to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Range window.	You must have at least one range specified for each criterion.
Add an Action	1. Select Action > Add in the Edit Filters window; then select the action to impose on packets that match any of the template's ranges of filtering criteria. 2. When you are finished adding actions to your template, click on OK.	With the exception of the Log action, each filter template has only one action. You can select Log in combination with any other action. Create new templates for additional actions.
Delete an Action	1. In the Filter Information scroll box, select the action to remove. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Action window.	There must be one at least action specified for a filter template.

4. **Click on OK when you are finished editing the template.**

   You return to the Filter Template Management window. You can continue to create, edit, or delete templates using this window.

5. **Click on Done to return to the Priority/Outbound Traffic Filters window.**

Creating an Outbound Filter

You create an outbound traffic filter by applying a filter template to an interface.

Note: Try to create the filters on each interface in order of precedence. The first filter you create has the highest precedence and a rule number of 1. Subsequent filters created on the interface have decreasing precedence. See “Changing Filter Precedence” for information on filter precedence.

To create a new filter:

1. **Display the Priority/Outbound Filters window (Figure 7-11).**

   See “Displaying the Priority/Outbound Filters Window” earlier in this chapter.

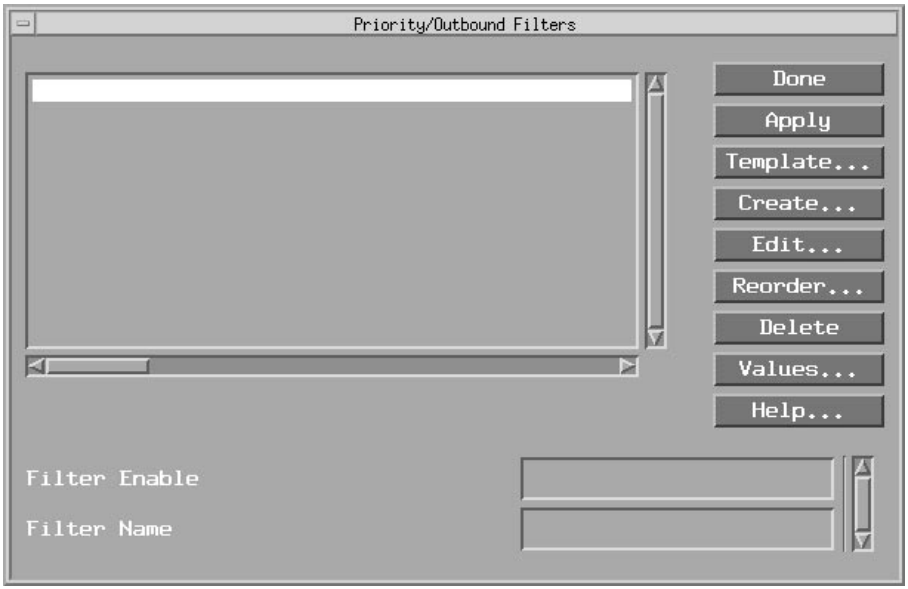

Figure 7-11. Priority/Outbound Filters Window

2. **Click on Create.**

   The Create Filter window appears (Figure 7-12).

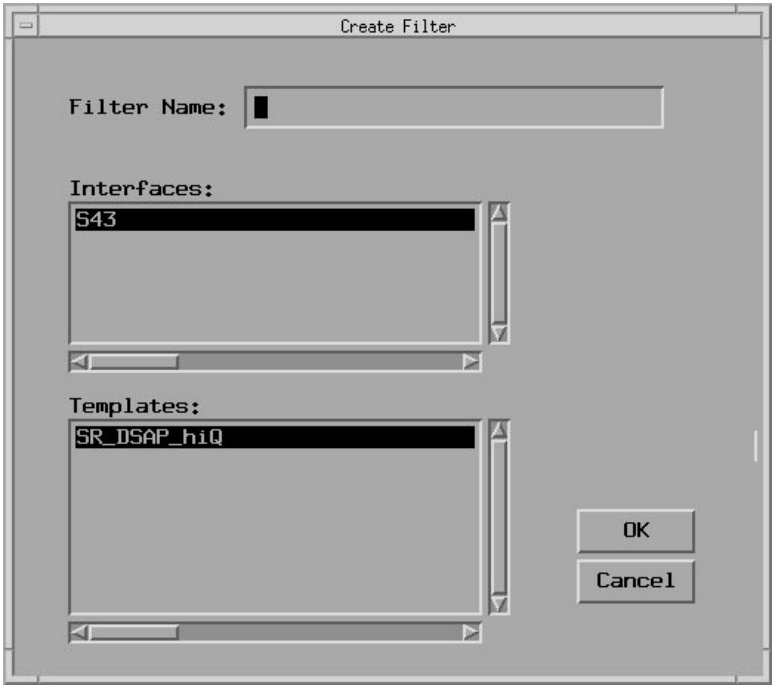

Figure 7-12. Create Filter Window

3. **If the correct interface is not already highlighted, select the interface.**
4. **Select the template you to use for the new filter.**

   Complete the steps in “Preparing Filter Templates” if the Templates box is empty.
5. **Type a name for the new filter in the Filter Name box.**
6. **Click on OK.**

   The Priority/Outbound Filters window reappears, with the new filter displayed in the scroll box.

Editing an Outbound Filter

After you apply a filter to an interface, you can edit its criterion, ranges, and actions. (However, if you used a template edited to suit your needs to create the filter, you probably don't need to make further edits.)

To customize an outbound traffic filter:

1. **Display the Priority/Outbound Filters window (refer to Figure 7-11).**
2. **In the scroll box, select the name of the filter you to edit.**
3. **Click on Edit.**

   The Edit Priority/Outbound Filters window appears (Figure 7-13).
4. **Use the Edit Priority/Outbound Filters window to add, change, or delete filter criteria, ranges, and actions as described in Table 7-2.**
5. **When you are finished editing the filter, select File > Save to exit.**

   The new filter information appears in the Filter Information scroll box in the Edit Priority/Outbound Filters window.

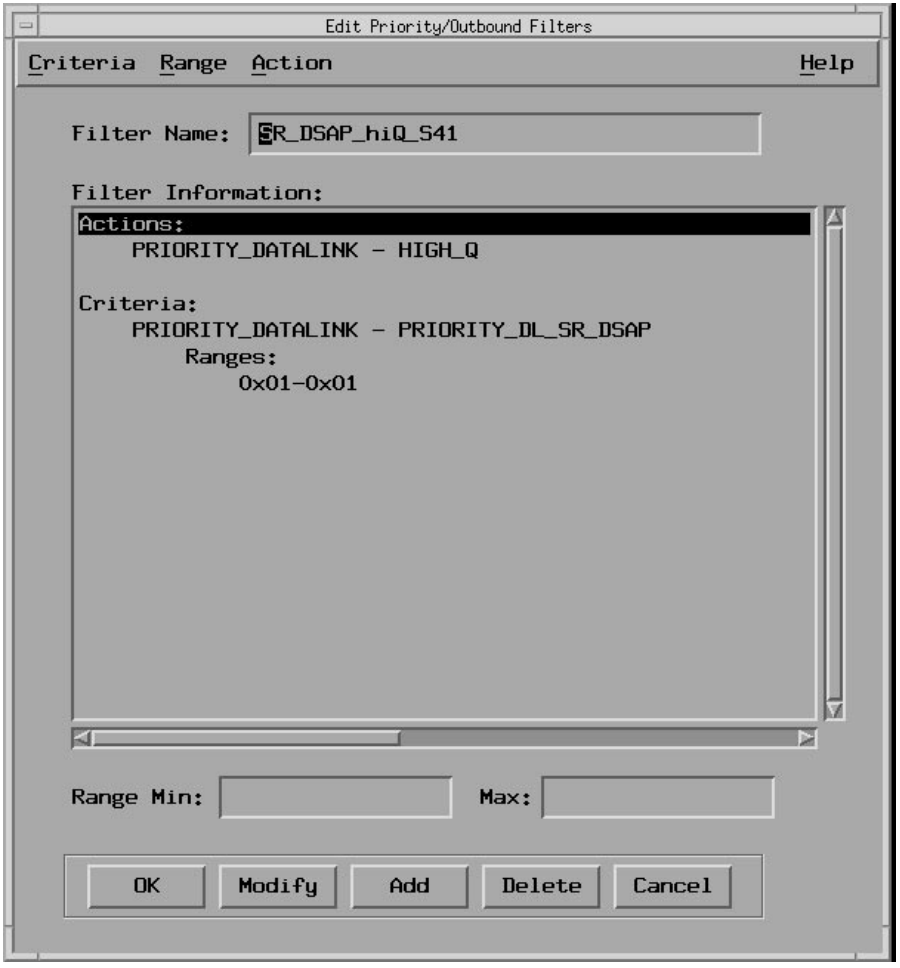

Figure 7-13. Edit Priority/Outbound Filters Window

Table 7-2. Using the Edit Priority/Outbound Filters Window

Task	Site Manager Instructions	Notes
Add a criterion	1. If the filter already has a criterion, delete that criterion. 2. Select Criteria > Datalink or IP > Add > *protocol header* > *filter criterion*. 3. Add a range in the Add Range window.	For any criterion you choose, you must specify at least one range. Each template can have only one criterion.
Delete a criterion	1. Select the criterion to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Criteria window.	Each filter template has only one criterion. Create new templates for additional criteria.
Add a range	1. Select the criterion in the Filter Information box. 2. Click on Add. 3. Use the Range Min and Max boxes to specify low and high values for the range.	You can add up to 100 ranges for each filter criterion. Use the prefix 0x to specify a hexadecimal number. To specify a range of just one value, specify that value in the Minimum value box. Zero is not a valid entry for minimum or maximum value.
Modify a range	1. Select the range to modify in the Filter Information box. 2. Click on Modify. 3. Use the Range Min and Max boxes to specify new low and high values for the range.	
Delete a range	1. Select the range to delete in the Filter Information scroll box. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Range window.	You must have at least one range specified for each criterion.
Add an Action	1. If the filter already has an action, delete that action. 2. Select Action→Add in the Edit Filters window; then select the action to impose on packets that match any of the template's ranges of filtering criteria. 3. When you are finished adding actions to your template, click on OK.	With the exception of the Log action, each filter template has only one action. You can select Log in combination with any other action. Create new templates for additional actions.
Delete an Action	1. In the Filter Information scroll box, select the action you to remove. 2. Click on Delete. 3. To confirm, click on Delete in the Delete Action window.	There must be one at least action specified for a filter template.

Changing Filter Precedence

You can assign as many as 31 outbound traffic filters per protocol to each router interface. As you add filters to an interface, the Configuration Manager numbers them chronologically (Filter No. 1, Filter No. 2, Filter No. 3, and so on). The number determines the filter precedence; lower rule numbers have higher precedence.

Figure 7-14 shows a sample listing of filters on an interface.

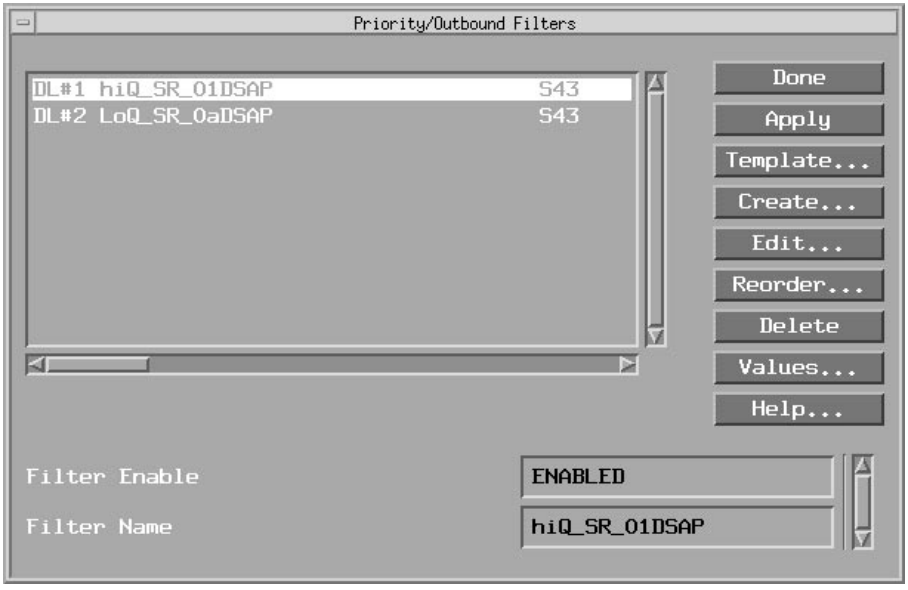

Figure 7-14. Sample List of Outbound Filters

The first filter has the highest precedence and the number 1. Subsequent filters created on the interface have decreasing precedence and increasing numbers. If a packet matches two filters, the filter with the highest precedence (lowest number) applies. For example, if the first filter on the interface (No. 1) drops a packet and the second filter (No. 2) accepts the same packet, Filter No. 1 has precedence and the packet will be dropped.

Try to create filters on the interface in order of precedence. However, if you can't, or if your filtering strategy changes, you can use the Priority/Outbound Filters window to rearrange the precedence of existing filters.

To change the order of precedence:

1. **In the Priority/Outbound Filters window (see Figure 7-14), select the filter for which you want to change the precedence.**
2. **Click on Reorder.**

   The Change Precedence window appears (Figure 7-15).

Figure 7-15. Change Precedence Window

3. **Click on either INSERT BEFORE or INSERT AFTER.**
4. **Type a number in the Precedence Number box to indicate which filter you should insert the selected filter before or after.**

   For the example shown, you place the selected filter (Filter No. 1) after Filter No. 2 by typing **1** in the Precedence Number box.
5. **Click on OK.**

   You are returned to the Priority/Outbound Filters window. The filters are now shown in their new order of precedence (Figure 7-16). Compare the order of filters in Figure 7-14 with the order in Figure 7-16.

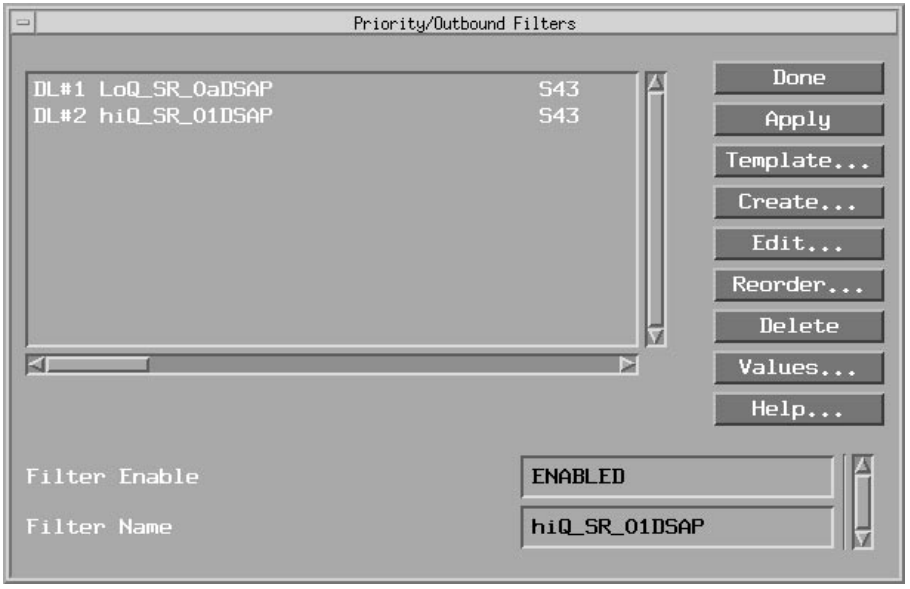

Figure 7-16. Example of Outbound Filter Order Change

Enabling or Disabling an Outbound Filter

You can disable and re-enable outbound filters on individual interfaces. When you do, only the filter on that interface is affected. To disable or re-enable a filter:

1. **Display the Priority/Outbound Filters window (refer to Figure 7-16).**
2. **Select a filter from the scroll box to disable or re-enable.**

   The current status of the selected filter appears in the Filter Enable and Filter Name boxes at the bottom of the window.
3. **Click on Values.**

   The Values window appears.
4. **Select ENABLED or DISABLED.**
5. **Click on OK.**
6. **Repeat the steps for each filter you to disable or re-enable.**
7. **Click on Done when you are finished.**

Deleting an Outbound Filter

To delete a priority or outbound filter from an interface:

1. **Display the Priority/Outbound Filters window (refer to Figure 7-16).**
2. **Select the outbound filter to delete.**
3. **Click on Delete.**

   The system deletes the filter from the interface, and the filter no longer appears in the outbound filters scroll box in the Priority/Outbound Filters window.

Caution: Do not click on Delete unless you are sure that you want to delete the selected filter. There is no way to confirm the deletion.

Appendix A
Site Manager Protocol Prioritization Parameters

This appendix contains reference information on Site Manager parameters

- Priority Interface Parameter Descriptions
- Prioritization Length Parameters

For each arameter associated with a physical-layer protocol, this appendix provides information about default settings, valid parameter options, the parameter function, instructions for setting the parameter, and the MIB object ID.

Priority Interface Parameter Descriptions

Use the following descriptions as guidelines when you edit parameters in the Edit Protocol Priority Interface window.

Parameter:	**Enable**
Path:	Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface
Default:	Enable
Options:	Enable | Disable
Function:	Toggles protocol prioritization on and off on this interface. If you set this parameter to Disable, all outbound filters will be disabled on this interface. Setting this parameter to Disable is useful if you want to temporarily disable all outbound filters rather than delete them.
Instructions:	Set to Disable if you want to temporarily disable all protocol prioritization activity on this interface. Set to Enable if you previously disabled protocol prioritization on this interface and now want to re-enable it.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.1.1.2

Parameter: High Queue Size

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 20 packets

Options: Any integer value

Function: Specifies the maximum number of packets in the high-priority queue at any one time, regardless of packet size.

Instructions: Accept the default or enter a new value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.4

Parameter: Normal Queue Size

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 20 (200 for Frame Relay)

Options: Any integer value

Function: Specifies the maximum number of packets in the normal-priority queue at any one time, regardless of packet size.

Instructions: Accept the default or enter a new value.

For Frame Relay interfaces, a value less than 200 might cause a broadcast message to be clipped.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.5

Parameter: Low Queue Size

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 20

Options: Any integer value

Function: Specifies the maximum number of packets in the low-priority queue at any one time, regardless of packet size.

Instructions: Accept the default of 20 packets or enter a new value.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.6

Parameter: Max High Queue Latency

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 250 milliseconds (ms)

Options: 100 to 5000 ms

Function: Specifies the greatest delay that a high-priority packet can experience and, consequently, how many normal-priority or low-priority bits can be in the transmit queue at any one time.

Instructions: Accept the default latency of 250 ms, or enter a new latency value. We recommend accepting the default latency value of 250 ms.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.8

Parameter: High Water Packets Clear

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 0

Options: Any integer value

Function: Toggles the High Water Packets Clear bit. When you change queue depth (by changing the value of the High Queue Size, Normal Queue Size, or Low Queue Size parameter) you can also reset the high water mark by changing the value of this parameter. When you change the value of this parameter, you reset the high water mark for all three queues to zero.

Instructions: Enter any new integer value for this parameter to clear the existing high water marks for the priority queues.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.19

Parameter: Prioritization Algorithm Type

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: BANDWIDTH ALLOCATION

Options: BANDWIDTH ALLOCATION | STRICT

Function: Selects the dequeuing algorithm that protocol prioritization uses to drain priority queues and transmit traffic. With strict dequeuing, the router always transmits traffic in the high-priority queue before traffic in the other queues. With bandwidth allocation dequeuing, the router transmits traffic in a queue until the utilization percentage for that queue is reached, and then the router transmits traffic in the next-lower-priority queue. (You configure the percentages for bandwidth allocation by setting the Hiqh Queue, Normal Queue, and Low Queue Percent Bandwidth parameters.)

Instructions: Accept the default of BANDWIDTH ALLOCATION or select STRICT.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.24

Parameter: High Queue Percent Bandwidth

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 70 percent

Options: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the percentage of the synchronous line's bandwidth allocated to traffic that has been sent to the high-priority queue. When you set this parameter to a value less than 100, each time the percentage of bandwidth used by high-priority traffic reaches this limit, the router transmits traffic in the normal- and low-priority queues, up to the configured percentages for those priority queues.

Instructions: Specify the percentage of the line's bandwidth allocated for high-priority traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.25

Parameter: Normal Queue Percent Bandwidth

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 20 percent

Options: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the percentage of the synchronous line's bandwidth that normal-priority traffic can use.

Instructions: Specify the percentage of the line's bandwidth allocated to normal traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.26

Parameter: Low Queue Percent Bandwidth

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: 10 percent

Options: 0 to 100 percent

Function: If you select the bandwidth allocation dequeuing algorithm, this parameter specifies the percentage of the synchronous line's bandwidth that low-priority traffic can use.

Instructions: Specify the percentage of the line's bandwidth allocated to low-priority traffic. The High Queue Percent Bandwidth, Normal Queue Percent Bandwidth, and Low Queue Percent Bandwidth values must total 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.26

Parameter: Discard Eligible Bit Low

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: ENABLE

Options: ENABLE | DISABLE

Function: Sets the Frame Relay Discard Eligible (DE) bit for packets sent to the Low priority queue. Sets the Frame Relay Discard Eligible (DE) bit for packets sent to the Low priority queue.

Instructions: Select DISABLE if you do not want the DE bit to be set for all Frame Relay packets in the Low priority queue.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.37

Parameter: Discard Eligible Bit Normal

Path: Configuration Manager > **Interface Connector** > **Edit Circuit** > Protocols > Edit Protocol Priority > Interface

Default: DISABLE

Options: ENABLE | DISABLE

Function: Sets the Frame Relay Discard Eligible (DE) bit for packets sent to the Normal priority queue.

By default, Frame Relay packets in the Normal priority queue do not have the Discard Eligible (DE) bit set.

Instructions:

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.1.1.38

Prioritization Length Parameters

Use the following descriptions as guidelines when you edit parameters in the Prioritization Length window.

Parameter: Packet Length

Path: Create Priority/Outbound Filters > Actions > Length > Prioritization Length

Default: None

Options: 0 to 4608 bytes

Function: Defines a packet length measurement to which each packet is compared. An action is imposed on every packet, depending on whether it is less than, equal to, or greater than the value you set for this parameter. This action also depends on the values of the Less Than or Equal Queue and the Greater Than Queue parameters.

Instructions: Enter a packet length value in bytes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.4.1.7

Parameter: Less Than or Equal Queue

Path: Create Priority/Outbound Filters > Actions > Length > Prioritization Length

Default: Normal

Options: High | Low | Normal

Function: Specifies which queue a packet is placed in if its packet length is less than or equal to the value of the Packet Length parameter. For example, if Packet Length is set to 1024 bytes, any packet that is 1024 bytes or smaller is placed in the queue you choose for this parameter.

Instructions: Accept the default, Normal, or select either Low or High.

MIB Object ID: 1.3.6.1.4.1.18.3.5.1.4.4.1.8

Parameter:	**Greater Than Queue**
Path:	Create Priority/Outbound Filters > Actions > Length > Prioritization Length
Default:	Low
Options:	High | Low | Normal
Function:	Specifies which queue a packet is placed in if its packet length is greater than the value of the Packet Length parameter. For example, if Packet Length is set to 1024 bytes, any packet that is 1025 bytes or larger is placed in the queue you choose for this parameter.
Instructions:	Accept the default, Low, or select either Normal or High.
MIB Object ID:	1.3.6.1.4.1.18.3.5.1.4.4.1.9

Appendix B
Examples and Implementation Notes

This appendix contains examples, hints, reminders, and important notes you could have missed earlier in this guide. Sections of this appendix provide

- Implementation Notes
- Inbound Traffic Filter Examples
- Protocol Prioritization Examples

Implementation Notes

This section contains notes about

- Filtering Outbound Frame Relay Traffic
- Filtering Over a Dial Backup Line
- Using a Drop-All Filter as a Firewall

Filtering Outbound Frame Relay Traffic

When creating outbound filters for Frame Relay traffic, keep in mind that Frame Relay packets in the Low priority queue have the Discard Eligible (DE) bit set by default. The DE bit is off by default in Frame Relay packets in the Normal and High priority queues.

You can change the default status of the DE bit for packets in the Low priority queue and the Normal priority queue in the Edit Protocol Priority Interface window. Refer to “Editing Protocol Prioritization Parameters” in Chapter 2 for instructions.

Filtering Over a Dial Backup Line

When configuring outbound filters or protocol prioritization on a synchronous interface on which you have configured a dial backup line, keep the following considerations in mind:

- If the primary line is running PPP and the line fails, the router automatically transfers all the priority queues and outbound filters you have configured on the primary line to the backup line.
- If the primary line is running a wide-area protocol other than PPP and the line fails, the router does *not* transfer Datalink protocol prioritization or outbound filters to the backup line. You must manually configure new Datalink outbound filters on the backup line after that line is activated.
- If the primary line is running a wide-area protocol other than PPP and the line fails, the router does transfer IP outbound filters to the backup line, no matter what protocol was running on the primary line.

Be careful when configuring outbound filters on the backup line. As soon as the primary line is reactivated, it uses the priority queues and filters you configured for the backup line. These priorities and filters may be completely inappropriate for the protocol running on the primary line.

Using a Drop-All Filter as a Firewall

If your filtering strategy involves forwarding most traffic and dropping only specified packets, you need only configure drop filters for the specific traffic you want the router to reject.

If your strategy involves blocking most traffic and accepting only specified packets (a “firewall”), begin by defining filters to accept specified packets. Then add a filter on the interface to drop all packets, a *drop-all filter.*

A drop-all filter describes the broadest range of packets you want to block from an interface. To ensure that all unwanted traffic gets dropped, configure the drop-all filter to contain

- Criteria that appears in *every* packet of the protocol you want to filter
- The maximum possible value of the range
- The minimum value of the range

With a drop-all filter specified, higher-precedence Accept filters create exceptions (or “holes”) in the drop-all range. Since the highest-precedence filter in a given address range determines the result of combined filtering within that range, the router processes packets that match the accept filters. However, the drop-all filter ensures the router rejects all other traffic.

For example, to configure a circuit that only accepts IP traffic addressed for destination address 192.32.28.55, apply a drop-all filter and one accept filter, as follows:

Filter Action	Rule Nunber	Start of Range	End of Range
Accept	1 (highest precedence)	192.32.28.55	192.32.28.55
Drop	2 (lower precedence)	0.0.0.0.0	255.255.255.255

See the “Changing Filter Precedence” sections in Chapter 6 (inbound filters) or Chapter 7 (outbound filters) for information about using the Configuration Manager to changing filter precedence after the filters are applied to an interface.

Inbound Traffic Filter Examples

You create a traffic filter by

1. Creating an Inbound Traffic Filter Template (Predefined Criteria)
   or
   Creating an Inbound Traffic Filter Template (User-Defined Criteria)
2. Applying the Traffic Filter Template.

If this section does not include an example for a protocol you want to configure, use these examples as guidelines for implementing inbound traffic filters for other traffic types.

Creating an Inbound Traffic Filter Template (Predefined Criteria)

This section provides examples for creating and applying a template with predefined criteria to:

- Drop inbound but allow outbound Telnet traffic
- Screen Telnet and FTP clients
- Customize BOOTP server operation

The following summarizes your steps for creating an inbound traffic filter template using a predefined criterion. Chapter 6 provides detailed procedures; Chapter 2 lists the predefined inbound traffic filter criteria and actions for all supported protocols, as well as the user-defined reference points for each protocol.

1. **Display the Traffic Filters window for your selected circuit.**
2. **Click on Template.**
3. **In the Filter Template Management window, click on Create.**

   The protocol-specific Create Filter Template window appears.
4. **Enter a descriptive name in the Filter Name box.**
5. **Select a criterion.**

   Refer to Table B-1 for specific examples.
6. **Enter one or more ranges.**

   Refer to Table B-1.
7. **Select an action.**

   Refer to Table B-1.
8. **Click on OK.**

   You are returned to the Filter Template Management window.
9. **Click on Done.**

   You are returned to the protocol-specific Traffic Filter window.
10. **Click on Create.**
11. **In the Create Filter window, enter a name for the filter.**
12. **Select the template file you just created in the Templates scroll box.**
13. **Click on OK.**

The filter is now applied to the selected interface.

Table B-1. Predefined Criteria, Ranges, and Actions for Example Inbound Traffic Filters

Filtering Goal	Criteria Path	Ranges	Action Path	Notes
Drop inbound Telnet traffic	Criteria > Add > IP > TCP Frame > TCP Destination Port	23 Refer to Table 5-6 in Chapter 5 for a list of common TCP destination port codes.	Action > Add > Drop	For a more secure method, create a user-defined filter (see the next section). This filter will not stop remote users from establishing a Telnet session with the router itself. To do that, set up a drop filter on the synchronous port with the same criterion, or create outbound filters on the remote links.
Configure a subset of allowed Telnet, TFTP, and FTP users	Criteria>Add> IP Source Address	Client addresses (Use dotted decimal format)	Action > Add > Accept	This strategy works only if the destination IP address is one of the router's interfaces and if the protocol or well-known port is Telnet, TFTP, or FTP.
Configure a router to drop BOOTP requests from particular clients	Criteria > Add > UDP Frame > UDP Destination Port	MAC addresses of BOOTP clients	Action > Add > Drop	

Creating an Inbound Traffic Filter Template (User-Defined Criteria)

This section describes how to create a template with user-defined criteria to

- Drop or accept VINES traffic bridged over an Ethernet interface
- Drop or accept DLSw traffic based on NetBIOS names
- Drop inbound (but allow outbound) Telnet traffic

The following summarizes your steps for creating an inbound traffic filter with a user-defined criterion. Chapter 6 provides detailed information.

Setting up user-defined criteria is similar to setting up predefined criteria, except you specify the criterion's location within the packet. Refer to Chapter 3 for the supported protocol header reference points you can use to specify user-defined inbound traffic filter criteria.

To specify user-defined criteria:

1. **Display the Traffic Filters window for your selected circuit.**
2. **Click on Template.**

   The Filter Template Management window appears.
3. **Click on Create.**

   The protocol-specific Create Filter Template window appears.
4. **Enter a descriptive name in the Filter Name box.**
5. **Select Criteria > Add > User-Defined.**

   The Add User-Defined Field window appears. In this window, you specify the criterion's

   - Reference Field
   - Offset
   - Length
   - Minimum Range
   - Maximum Range
6. **Select the protocol-specific reference field.**

   Refer to Table B-2 for specific examples.
7. **Specify an offset and length from the reference field.**

   Refer to Table B-2.
8. **Specify a range.**
9. **Click on OK.**
10. **Select an Action.**
11. **Click on OK.**

    You are returned to the Filter Template Management window.
12. **Click on Done.**

    The protocol-specific Traffic Filter window re-appears.

Table B-2. User-Defined Criteria and Ranges for Example Inbound Traffic Filters

Filtering Goal	User-Defined Criteria			Range
	Reference Field	**Offset**	**Length**	
Give certain VINES traffic that is bridged over Ethernet precedence over all other traffic	Specify an Ethernet Type field of 0xBAD (VINES)	160 bits (sum of all criteria that precede the Destination Network field, or 48+48+16+16+16+8+8)	32 bits	Specify the hexadecimal destination network number (for example, 1234).
On a DLSw circuit, filter on NetBIOS Names.	DLS_DATA_START	376 (Destination NetBIOS Names) 504 (Source NetBIOS Names) The offset of 376 only applies if you want to filter the beginning of the NetBIOS name field. If you want to find a particular section of the NetBIOS name, the offset will increase by X * 8, where X is the number of bytes into the name that you want to filter.	NetBIOS names are up to 16 bytes long. How they are oriented in the field (right justified or left justified) may be dependent on application and should be checked with an analyzer before creating filter criteria.	Enter NetBIOS Name ranges, using the ASCII equivalent of the first 15 characters in the name. For names with less than 15 characters, use 0x20 to pad characters .
Drop inbound Telnet and FTP traffic on the synchronous interface that receives packets from the Internet.	IP HEADER_END	107 109	1	0x0 - 0x0

Applying the Traffic Filter Template

Create a traffic filter by applying a filter template to an interface:

1. **Begin at the protocol-specific Traffic Filter window**
2. **Click on Create.**
3. **In the Create Filter window, enter a name for the filter.**
4. **Select the template file you just created in the Templates scroll box.**
5. **Click on OK.**

   The filter is now applied to the selected interface.

Protocol Prioritization Examples

This section provides summary examples for configuring protocol priority queues for the following traffic:

- LAT
- ICMP
- SNA
- DLSw
- RIP
- OSPF and OSPF/BGP
- Spanning Tree
- Sync Pass-through
- FTP
- Source Routing

If this section does not include an exact example for a protocol you want to configure, use these examples as guidelines for implementing protocol prioritization for other traffic types.

To create an outbound traffic filter with a queue action:

1. **Display the Priority/Outbound Filter window.**
2. **Click on Template.**

   The Filter Template Management window appears. The Templates scroll box includes any existing filter templates.
3. **Click on Create.**

   The Create Priority/Outbound Template window appears.
4. **Enter a descriptive name for the new template in the Filter Name box.**
5. **Select a criterion.**

   Refer to Table B-3 for specific examples.
6. **Enter a range.**

   Refer to Table B-3.
7. **Select a queue action.**

   Refer to Table B-3.
8. **Click on Done.**

   The Priority/Outbound Filters window reappears.
9. **Click on Create.**

   The Create Filter window appears.
10. **Select an interface.**
11. **Select the template file.**
12. **Enter a descriptive name for the filter.**
13. **Click on OK.**

    The filter is now applied to the selected interface.

Table B-3. Example Criteria, Ranges, and Actions for Protocol Prioritization

Filtering Goal	Criteria Path	Ranges	Action Path	Notes
Place LAT traffic in the high priority queue (since LAT is a time-sensitive protocol)	Criteria > Add > Datalink > Datalink type > Ethernet type NOTE: If this is a Frame Relay interface, specify SNAP instead of Ethernet type).	6004	Action > Datalink > Add > High Queue	Table 5-8 in Chapter 5 includes a list of common Ethernet type codes.
Place ICMP traffic in the low priority queue (ICMP is not a time-sensitive protocol)	CriteriaAdd > IP > IP > Protocol	1	Action > IP > Add > Low Queue	Table 5-9 in Chapter 5 includes a list of some common IP Protocol codes.
Place SNA traffic in the high priority queue	Criteria > Add > Data link > Source Routing > DSAP NOTE: To prioritize IP-encapsulated SNA traffic, select Criteria > Add > IP > Source Routing > DSAP	DSAP values: 0x04 to 0x05 0x08 to 0x09 0x0c to 0x0d See Chapter 5 for information on specifying MAC address or SAP criteria ranges.	Action > Datalink > Add > High Queue NOTE: To prioritize IP-encapsulated SNA traffic, select Action > IP > Add > High Queue	You can also select SSAP, Destination MAC address, or Source MAC address as the criteria.
Place all DLSw traffic leaving particular a synchronous interface in the high priority queue	Criteria > Add > IP > IP > TCP Destination Port	2065 to 2067 Refer to Table 5-6 in Chapter 5 for a list of common TCP destination port codes.	Action > IP > Add > High Queue	This example shows how to prioritize DLSw traffic before other protocols on the interface. To affect the priority of specific types of DLSw traffic at the TCP level, use DLSw protocol prioritization as described in *Configuring DLSw Services*.

(continued)

Table B-3. Example Criteria, Ranges, and Actions for Protocol Prioritization

Filtering Goal	Criteria Path	Ranges	Action Path	Notes
Place RIP traffic in the low priority queue.	Criteria > Add > IP > IP > UDP Destination Port	520	Action > IP > Add > Low Queue	Refer to Table 5-7 in Chapter 5 for a list of common UDP destination port codes.
Place OSPF traffic in the high priority queue	Criteria > Add > IP > IP > Protocol Type	89	Action > IP > Add > High Queue	Refer to Table 5-9 in Chapter 5 for a list of common IP Protocol codes.
Place OSPF/BGP traffic in the high priority queue.	Criteria > Add > IP > IP > Type of Service	0xe0	Action > IP > Add > High Queue	
Place Spanning Tree traffic in the high priority queue	Criteria > Add > Datalink > Source Routing > DSAP | SSAP | Control	0x42 (DSAP or SSAP) 0x03 (Control code)	Action > Datalink > Add > High Queue	Refer to Table 5-3 in Chapter 5 for a list of SAP codes.
Place synchronous pass-through traffic in the high priority queue	Criteria > Add > Datalink > 802.2 SNAP Ethernet	0x80FF	Action > Datalink > Add > High Queue	
Prioritize FTP, Telnet, and other large-packet data traffic by placing smaller packets in the low priority queue	Criteria > Add > IP > Source Address	Client addresses	Action > IP > Add > Length	In the Prioritization Length window, specify: Packet Length = 500 bytes Less Than or Equal Queue = Low Greater Than Queue = High

Index

A

accept filters, 1-6, B-2, B-3

actions, traffic filter. *See* traffic filter actions.

adding
- actions
  - inbound, 6-14, 6-19
  - outbound, 7-14, 7-17, 7-19
- criteria
  - inbound, 6-14, 6-19
  - outbound, 7-14, 7-17, 7-19
- ranges, 5-1 to 5-10

applying templates
- inbound traffic filter, 6-15
- outbound traffic filter, 7-15

APPN, 3-12

B

bandwidth allocation dequeuing algorithm, 2-2

Bay Networks
- CompuServe forum, xxii
- Customer Service FTP, xxi
- home page on World Wide Web, xxi
- InfoFACTS service, xxiii
- publications, ordering, xviii
- support programs, xx
- Support Source CD, xxii
- Technical Response Center, xix, xxiii
- technical support, xix

blocking filters, 1-6, B-2

Bridge, Source Route
- actions
  - inbound, 3-6
  - outbound, 4-9
- criteria
  - inbound, 3-5 to 3-6
  - outbound, 4-2
- ranges, 3-5

Bridge, Transparent
- actions
  - inbound, 3-4
  - outbound, 4-9
- criteria
  - inbound, 3-2 to 3-4
  - outbound, 4-2

C

Clipped Packets Count, 2-8

clock speed, 2-3

CompuServe, Bay Networks forum on, xxii

configuring
- inbound traffic filters, 6-1
- outbound traffic filters, 7-1

criteria, inbound traffic filter
- 802.2
  - Control, 3-3
  - DSAP, 3-3
  - Length, 3-3
  - SSAP, 3-3
- adding, 6-14, 6-19
- Bridge, Transparent
  - 802.2, 3-3
  - Ethernet type, 3-3
  - MAC Destination Address, 3-3
  - MAC Source Address, 3-3
  - Novell, 3-3
  - SNAP, 3-3

- DECnet Phase IV
  - Destination Area, 3-7
  - Destination Node, 3-7
  - Source Area, 3-7
  - Source Node, 3-7
- defined, 1-8, 3-1
- deleting, 6-14, 6-19
- DLSw
  - Destination MAC Address, 3-8
  - DSAP, 3-8
  - Source MAC Address, 3-8
  - SSAP, 3-8
- IP
  - IP Destination Address, 3-9
  - IP Source Address, 3-9
  - Protocol, 3-9
  - TCP Destination Port, 3-9
  - TCP Source Port, 3-9
  - Type of Service, 3-9
  - UDP Destination Port, 3-9
  - UDP Source Port, 3-9
- IPX
  - Destination Address, 3-11
  - Destination Network, 3-11
  - Destination Socket, 3-11
  - Source Address, 3-11
  - Source Socket, 3-11
- LLC2
  - Destination MAC Address, 3-12
  - DSAP, 3-12
  - Source MAC Address, 3-12
  - SSAP, 3-12
- OSI
  - Destination Area, 3-13
  - Destination System ID, 3-13
  - Source Area, 3-13
  - Source System ID, 3-13
- SNAP
  - Ethertype, 3-3
  - Length, 3-3
  - Protocol ID/Organization Code, 3-3
- Source Routing
  - Destination MAC Address, 3-5
  - Destination NetBIOS Name, 3-5
  - DSAP, 3-5
  - Next Ring, 3-5
  - Source MAC Address, 3-5
  - Source NetBIOS Name, 3-5
  - SSAP, 3-5
- user-defined, 6-20 to 6-21
- VINES
  - Destination Address, 3-14
  - Protocol Type, 3-14
  - Source Address, 3-14
- XNS
  - Destination Address, 3-15
  - Destination Network, 3-15
  - Destination Socket, 3-15
  - Source Address, 3-15
  - Source Socket, 3-15

criteria, outbound traffic filter
- adding, 7-14, 7-17, 7-19
- common headers, 4-5
- Data Link header, 4-2
- defined, 1-8, 4-1
- deleting, 7-14, 7-19
- IP header, 4-4
- user-defined, 4-6 to 4-8

Customer Service FTP, xxi

customer support. *See* getting help

D

Data Link header
- outbound traffic filter criteria, 4-2
- reference points, 4-6

DECnet
- actions, 3-7
- criteria, 3-7

deleting
- inbound traffic filters, 6-26
- outbound traffic filters, 7-23

deleting actions
inbound traffic filter, 6-14, 6-19
outbound traffic filter, 7-14, 7-19
deleting criteria
inbound traffic filter, 6-14, 6-19
outbound traffic filter, 7-14, 7-19
deleting ranges
inbound traffic filter, 6-14, 6-19
outbound traffic filter, 7-14, 7-19
dequeuing algorithms
bandwidth allocation, 2-2
strict dequeuing, 2-6
Detailed Log action, 4-9
Detailed Logging action, 3-10
dial backup line, filters on, B-2
Direct IP Explorers action, 3-6
disabling
inbound traffic filters, 6-24
outbound traffic filters, 7-22
Discard Eligible Bit Low parameter, 2-21, A-6
Discard Eligible Bit Normal parameter, 2-21, A-6
DLSw
actions, 3-8
criteria, 3-8
example, B-10
Drop if Next Hop is Unreachable action, 3-10
drop traffic strategy, 1-6
drop-all filters, 1-6, B-2

E

editing
inbound traffic filters, 6-17
outbound traffic filters, 7-17
enabling
inbound traffic filters, 6-24
outbound traffic filters, 7-22
Ethernet Type ranges
Frame Relay traffic, 5-4, 5-7
IPX over Frame Relay traffic, 5-9
examples
DLSw, B-10
FTP, B-11
ICMP traffic, B-10
LAT, B-10
NetBIOS names, B-7
OSPF, B-11
OSPF traffic, B-11
protocol prioritization, B-1
RIP traffic, B-11
SNA, B-10
Spanning Tree, B-11
synchronous pass-through, B-11
Telnet, B-11

F

filter templates. *See* templates
firewall strategy, 1-6, B-2
Flood action, 3-4
Forward action, 3-10
Forward to Circuit List action, 3-4, 3-6
Forward to First Up Next Hop Interface action, 3-10
Forward to IP Address action, 3-10
Forward to Next Hop Interfaces action, 3-10
Forward to Peer action, 3-8
Frame Relay
Normal Queue size, 2-18, A-2
specifying Ethernet Type code, 5-4, 5-7
FTP traffic, prioritizing, B-11

G

getting help
from a Bay Networks Technical Response Center, xxiii
from the Support Source CD, xxii
through CompuServe, xxii
through Customer Service FTP, xxi
through InfoFACTS service, xxiii
through World Wide Web, xxi

Greater Than Queue parameter, 7-10, A-8

H

High Queue action, 1-14, 4-9
High Queue Percent Bandwidth parameter, 2-20, A-4
High Water Packets Clear parameter, 2-19, A-3
High-Water Packets Mark, 2-8

I

ICMP traffic, example, B-10
InfoFACTS service, xxiii
IP
  criteria, ?? to 3-9
  inbound
    actions, 3-10
    criteria, 3-9
  outbound traffic filters, 4-4
IP header
  outbound traffic filters, 4-8
  reference points, 4-8
IPX
  actions, 3-12
  criteria, 3-11
  specifying Ethernet Type code, 5-9

L

LAN Network Manager (LNM), 3-12, 5-4
LAT filter example, B-10
latency, 2-12
Length action, 1-14, 4-9
Less Than or Equal Queue parameter, 7-10, A-7
line delay, 2-12
LLC2
  actions, 3-12
  criteria, 3-12
Low Queue Percent Bandwidth parameter, 2-21, A-5
Low Queue Size parameter, 2-18, A-2

M

Max High Queue Latency parameter, 2-19, A-3
modifying ranges
  inbound traffic filter, 6-14, 6-19
  outbound traffic filter, 7-14, 7-17, 7-19

N

naming templates
  inbound traffic filter, 6-7
  outbound traffic filter, 7-6
NetBIOS filter example, B-7
NetBIOS Name, specifying range, 3-5
NetBIOS traffic, 4-2
No Call action, 1-14, 4-10
Normal Queue Percent Bandwidth parameter, 2-20, A-5
Normal Queue Size parameter, 2-18, A-2

O

OSI
  actions, 3-13
  criteria, 3-13
OSPF traffic, prioritizing, B-11
OSPF/BGP traffic, prioritizing, B-11

P

Packet Length parameter, 7-10, A-7
parameters, Protocol Prioritization
  Discard Eligible Bit Low, 2-21, A-6
  Discard Eligible Bit Normal, 2-21, A-6
  Enable, 2-18, A-1
  Greater Than Queue, 7-10, A-8
  High Queue Percent Bandwidth, 2-20, A-4
  High Queue Size, 2-18, A-2

High Water Packets Clear, 2-19, A-3
Less Than or Equal Queue, 7-10, A-7
Low Queue Percent Bandwidth, 2-21, A-5
Low Queue Size, 2-18, A-2
Max High Queue Latency, 2-19, A-3
Normal Queue Percent Bandwidth, 2-20, A-5
Normal Queue Size, 2-18, A-2
Packet Length, 7-10, A-7
Prioritization Algorithm Type, 2-19, A-4
performance, 1-6
precedence
and drop-all filters, B-2
inbound traffic filters, 6-22
outbound traffic filters, 7-20
predefined criteria, about, 1-8
Prioritization Algorithm Type parameter, 2-19, A-4
prioritization, protocol. *See* protocol prioritization
protocol prioritization
clipped packets, 2-8
defined, 1-4
dequeuing algorithms
bandwidth allocation, 2-2
strict dequeuing, 2-6
Discard Eligible Bit Low parameter, 2-21, A-6
Discard Eligible Bit Normal parameter, 2-21, A-6
DLSw
Inbound Traffic Filters window, 6-3
editing interface parameters, 2-15
Enable parameter, 2-18, A-1
enabling, 2-12
examples, B-10
Frame Relay, 2-18, A-2
Greater Than Queue parameter, 7-10, A-8
High Queue Percent Bandwidth parameter, 2-20, A-4
High Queue Size parameter, 2-18, A-2
High Water Packets Clear parameter, 2-19, A-3
HiWater packets mark, 2-8
how it works, 2-2
latency, 2-12
Less Than or Equal Queue parameter, 7-10, A-7
Low Queue Percent Bandwidth parameter, 2-21, A-5
Low Queue Size parameter, 2-18, A-2
Max High Queue Latency parameter, 2-19, A-3
Normal Queue Percent Bandwidth parameter, 2-20, A-5
Normal Queue Size parameter, 2-18, A-2
outbound traffic filters, 7-1
Packet Length parameter, 7-10, A-7
Prioritization Algorithm Type parameter, 2-19, A-4
protocols supported, 2-1
queue depth, 2-10
tuning, 2-12
usefulness of, 1-3

Q

queue depth, 2-10
queues, priority (High, Normal, Low). *See* protocol prioritization, 2-2

R

ranges
inbound traffic filter
changing, 6-14, 6-19
defined, 3-1
deleting, 6-14, 6-19
outbound traffic filter
changing, 7-14, 7-17, 7-19
deleting, 7-14, 7-19
specifying
NetBIOS Name, 3-5
SRB, 3-5
VINES, 5-3

reference points
Data Link header, 4-6
DECnet Phase IV, 3-7
DLSw, 3-8
IP header
inbound filters, 3-9
outbound filters, 4-8
IPX, 3-11
LLC2, 3-12
OSI, 3-13
Source Routing, 3-6
Transparent Bridge, 3-2
VINES, 3-14
XNS, 3-14
RIP traffic, prioritizing, B-11

S

SNA traffic, 4-2
SNA traffic, example, B-10
source routing
actions, 3-6, 4-9
criteria, 4-2
inbound, 3-5, 3-6
ranges, 3-5
Spanning Tree traffic, prioritizing, B-11
strict dequeuing algorithm, 2-6
Support Source CD, xxii
synchronous pass-through traffic, prioritizing, B-11

T

TCP Port criteria, 5-5
Telnet traffic, prioritizing, B-11
templates, about, 1-15 to 1-16
templates, inbound traffic filter
applying to an interface, 6-15
copying, 6-12
creating, 6-5
deleting criteria, 6-14, 6-19
deleting ranges, 6-14, 6-19
editing, 6-12
naming, 6-7
renaming, 6-13
templates, outbound traffic filter
copying, 7-11
creating, 7-4
deleting actions, 7-17
deleting criteria, 7-14, 7-17, 7-19
deleting ranges, 7-14, 7-19
editing, 7-11
naming, 7-6
renaming, 7-12
traffic filter actions
Accept, 1-13, 4-9
defined, 1-13
Drop, 1-13, 4-9
High Queue, 1-14, 4-9
inbound
adding, 6-14, 6-19
Bridge, 3-4
DECnet Phase IV, 3-7
deleting, 6-14, 6-19
DLSw, 3-8
IP, 3-10
IPX, 3-12
LLC2, 3-12
OSI, 3-13
source routing, 3-6
VINES, 3-14
XNS, 3-15
Length, 1-14, 4-9
Log, 1-13, 4-9
Low Queue, 1-14, 4-9
No Call, 1-14, 4-10
No Reset, 1-14, 4-10
outbound
adding, 7-14, 7-17, 7-19
Bridge, 4-9
deleting, 7-14, 7-19
deleting from a template, 7-17
source routing, 4-9

traffic filters
about, 1-1
actions, 1-13
adding to an interface, 1-15
blocking strategy, B-2
components of, 1-7
drop-all, B-2
dropping strategy, B-2
forwarding strategy, B-2
inbound
adding to an interface, 6-15
creating, 6-15
creating templates, 6-4
defined, 1-1
deleting from an interface, 6-26
DLSw, 6-3
enabling, 6-24
media and protocols supported, 1-2
precedence, 6-22
outbound, 7-1
adding to an interface, 7-15
creating templates, 7-3
defined, 1-1
deleting, 7-23
disabling, 7-22
editing, 7-17
enabling, 7-22
High Queue action, 1-14, 4-9
Length action, 1-14, 4-9
Low Queue action, 1-14, 4-9
media and protocols supported, 1-3
No Call action, 1-14, 4-10
No Reset action, 1-14, 4-10
precedence, 7-20
reordering, 7-20
precedence, 1-7, B-2
purpose of, 1-5
ranges, 1-12
strategies, 1-6
templates, 1-15 to 1-16
Transparent Bridge. *See* Bridge.

U

UDP Port Criteria, 5-5
user-defined criteria
about, 1-8
components of, 1-8
inbound
Bridge, 3-4
DECnet, 3-7
DLSw, 3-8
IP, 3-9
IPX, 3-11
LLC2, 3-12
OSI, 3-13
specifying, 6-20, 6-20 to 6-21
SRB, 3-6
VINES, 3-14
XNS, 3-15
outbound, 4-6 to 4-8

V

VINES
actions, 3-14
criteria, 3-14
ranges, 5-3

W

World Wide Web, Bay Networks home page on, xxi

X

XNS
actions, 3-15
criteria, 3-15